PMI-110-F2G

User's Manual

Version 1.0

Industrial Managed

PoE Switch

©Westermo Teleindustri AB

Copyright Notice

Copyright © 2014 Westermo Teleindustri AB

All rights reserved.

Reproduction in any form or by any means without permission is prohibited.

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his expense.

The user is cautioned that changes and modifications made to the equipment without approval of the manufacturer could void the user's authority to operate this equipment.

Index

1 Introduction....2
1.1 Overview....2
1.2 Major Features....5
1.3 Package List....6
2 Hardware Installation....7
2.1 Hardware Introduction....8
2.2 Wiring Power Inputs....12
2.3 Wiring the Relay Output (DO)....13
2.4 Wiring the Digital Input (DI)....14
2.5 Connecting the Surge /Lighting protection....15
2.6 Wiring Fast Ethernet PoE Ports....15
2.7 DIN Rail mounting Installation....17
3 Preparation for Management....19
3.1 Preparation for Serial Console....19
3.2 Preparation for Web Interface....20
3.3 Preparation for Telnet Console....22
4 Feature Configuration....25
4.1 Command Line Interface Introduction....26
4.2 Basic Setting....33
4.3 Port Configuration....49
4.4 Power over Ethernet....56
4.5 Network Redundancy....64
4.6 VLAN....84
4.7 Private VLAN....93
4.8 Traffic Prioritization....99
4.9 Multicast Filtering....105
4.10 SNMP....110
4.11 Security....114
4.12 Warning....121
4.13 Monitor and Diag....129
4.14 Device Front Panel....136
4.15 Save to Flash....137
4.16 Logout....138
5 Appendix....139
5.1 Pin assignment of RS-232 serial console cable....139

5.2 Westermo Private MIB 140
5.3 Revision History 141

1 Introduction

Welcome to Westermo *PMI-110-F2G* Series Industrial 8-Port PoE + 2Gigabit Copper / SFP Managed Ethernet Switch User Manual. Following topics are covered in this chapter:

1.1Overview

1.2Major Features

1.3Package Checklist

1.1 Overview

Westermo PMI-110-F2G is designed with eight 10/100TX PoE injector ports and two Gigabit RJ-45 / SFP combo ports for highly critical PoE applications such as real time IP video surveillance, WiMAX systems and Wireless APs. All of the 8 ports of the switch are compliant with both IEEE 802.3af PoE and IEEE 802.3at high power PoE standards and can deliver up to 15.4W and 30W power per port to enable the high-power requiring devices, such as Wireless APs, PTZ and dome network cameras, etc.

The two Gigabit Ethernet combo ports provide high speed uplink to connect with higher level backbone switches with network redundancy technology, while ensuring the reliability of video transfer through the exclusive 5ms recovery time. By supporting various connection types, including 10/100/1000Mbps RJ-45 copper or 100Mbps, 1000Mbps Fiber, the Gigabit uplink ports further enlarge the ring infrastructure.

With IEC 61000-6-2 / 61000-6-4 Heavy Industrial EMC certified design, including robust enclosure and -40~70°C wide operating temperature range, PMI-110-F2G ensures high performance in harsh surveillance applications.

Driving the IP Surveillance Market

Since the ratification of the Power over Ethernet standard in 2003, the PoE technology becomes a trend; more devices adopt PD function to obtain power through Ethernet cable eliminating the need of running separate power wirings to a remote device. The PMI-110-F2G is equipped with the new PSE solution, compliant with **IEEE 802.3af**, **IEEE 802.3at 2-event** or **IEEE 802.3at 2-event plus LLDP** standards, as well as forced mode powering mode for legacy Power over Ethernet cable devices. The 8 PoE ports support LLDP power negotiation function or 2-Event classification of IEEE 802.3at PoE plus, and can therefore deliver up to 30W power per port and 120W per unit at 70°C operating temperature, to drive the IP cameras for cross-street monitoring or WiMAX systems for internet accesses at train stations, airports or Hot-spots.

100/1000Mbps DDM SFP transceiver for High Quality Monitoring

The SFP sockets of the PMI-110-F2G supports 100Mbps and 1000Mbps SFP type fiber transceiver with speed detection and independent indication. Moreover, it supports DDM (Digital Diagnostic Monitoring) type SFP transceivers allowing users to diagnose optical cable transmission problem through maintenance and debugging of the optical signal quality by DDM without the need of an extra optical cable analyzer, as a result greatly saving time and system costs.

Rapid Super Ring (RSR) Technology

The PMI-110-F2G supports Rapid Super Ring technology. The recovery time is greatly improved from 30ms to few ms for both copper and fiber ring. The Ring master can be auto-selected by RSR engine. The 1st ring port of the R.M. is the primary path while the 2nd ring port of the R.M. is the block path. Once the primary path fails, the 2nd path will be recovered within few ms. Besides, the restoration time is also shortened to zero in the R.M. auto-selection mode.

Comprehensive Redundant Solutions – Multiple Super Ring (MSR)

PMI-110-F2G also supports advanced Ring technology – M.S.R. (Multiple Super Ring) which includes various new technologies for different network redundancy applications and structures. The supported MSR allows PMI-110-F2G aggregating up to 5 Rapid Super rings includes 4 Fast Ethernet plus 1 Gigabit Ethernet rings into one switch. With the MSR technology, a node can be configured to multiple rings with the failover time. In addition, users can extend the ring topology by adding hundreds of PMI managed switches to meet the large-scale network needs without compromising the network speed. The MSR also allows PMI-110-F2G managed switch to easily connect with core management switches via standard Rapid Spanning Tree Protocol (RSTP) or through multiple paths or nodes to increase the reliability by RDH (Rapid Dual Homing) technology. By integrating MSR and LACP (Link Aggregation Control Protocol), the PMI series can enhance the link ability and increase the overall link capacity. Two or more Fast Ethernet connections are combined in order to increase the bandwidth and to create a resilient and redundant link.

Seamless Ring Port Restoration

Seamless restoration is a new patented technology which can restore a failed ring without causing any loop problem, topology change and packet loss. With a 0 second restoration time, this mechanism eliminates any unstable status and guarantees the applications running non-stop.

Rapid Dual Homing (RDH) Technology

Rapid Dual Homing is also the important feature of new generation Ring technology. It supports ring coupling with other vendors and with easy configuration and multiple redundancies, the failover time is much faster and the restoration time is zero ms. Uplinks can be auto detected and gathered into groups. In each group, uplinks are sorted into primary, secondary and standbys by their link speed. The uplink with the highest speed is more likely to be active path for data transmission. Link aggregation is also integrated into RDH. An uplink connection can be a single link or several links aggregated as a trunk, which provides better redundancy and link capacity.

TrunkRing

TrunkRing is a new feature in MSR which merges the two technologies of RSR and link aggregation. It takes advantages of aggregation to enhance the link redundancy, while increase the link speed. The ring will open only if all the aggregated links are broken. Link aggregation can be achieved by either, static trunk or LACP. Not all the link sections in a TrunkRing need to be the same. Ring links can be either symmetric or asymmetric. Some are a single path, and the others are aggregated by links where the number of links in a trunk group can be different. Users can enhance the link redundancy at different locations in accordance to the need. And the link with less speed is more likely to be used as the backup path for restoring the network to full play capacity.

Link Aggregation Control Protocol

Link Aggregation Control Protocol allows you grouping multiple Ethernet ports in parallel to increase the link bandwidth. The aggregated ports can be viewed as one physical port, so that the bandwidth is higher than just one single Ethernet port. The member ports of the same trunk group can balance the loading and backup with each other. The LACP feature is usually used when you need higher bandwidth for the backbone network. This is a cost-effective way for you to transfer much more data.

Multi Powering Mechanism- User Manual, Forced and IEEE 802.3at LLDP Power over Ethernet

Some of Legacy PD devices also feature user defined manual mode and forced powering mode to support non-standard PD devices without the PoE signature resistor for some WiMax systems, which are non-compliant with IEEE 802.3at LLDP Power over Ethernet.
For the new PoE standard – IEEE 802.3at, PMI Switch implements Link Layer Discovery Protocol (LLDP) into the system for allowing power budget negotiation between PD devices while providing smart power budget control behavior.

Outstanding Management and Enhanced Security

The PMI-110-F2G provides various network control and security features to ensure the reliable

and secure network connection. To optimize industrial network environment the switch supports advanced network features, such as Tag VLAN, IGMP Snooping, Quality of Service (QoS), Link Aggregation Control Protocol (LACP), Rate Control, etc. The PoE switch can be smartly configured through WeDashboard, Web Browser, SNMP, Telnet and RS-232 local console with its command like interface. The failure notifications are sent through e-mail, SNMP trap, Local/Remote system log, Multiple event alarm relay.

To avoid hacker's attacks and ensure the secure data transmission, PMI-110-F2G series features DHCP client, DHCP server with IP and MAC binding, 802.1X Access Control, SSH for Telnet security, IP Access table, port security and many other security features.

1.2 Major Features

Westermo PMI-110-F2G Switch have following features:

- 8 10/100 Base TX PoE ports and 2 Gigabit RJ/ SFP combo ports
- IEEE 802.3af 15.4W / IEEE 802.3at 30W High Power PoE
- 120W total power budget for High-power PoE camera
- SFP ports support 100/1000 Mbps with Digital Diagnostic Monitoring (DDM) to monitor long distance fiber quality
- All ports support 5ms recovery time, and MSR for up to 4 x 100M Rings plus 1 Gigabit Ring
- Advanced management by LACP/VLAN/Q-in-Q/Private VLAN/ GVRP/ QoS/ IGMP Snooping/Rate Control/ Online Multi-Port Mirroring/ Advanced DHCP server, Client
- Advanced Security system by Port Security, Access IP list, SSH and HTTPS Login
- Event Notification through E-mail, SNMP trap and SysLog
- Supports console CLI , Web, LLDP, SNMP, RMON, and WeDashboard for remote management
- Multiple event relay output for enhanced device alarm control
- Hi-Pot Isolation Protection for ports and power
- Industrial Heat dispersing design, -40~70˚C wide operating temperature

1.3 Package List

Westermo PMI-110-F2G is shipped with following items:

- PMI-110-F2G
- One DIN-Rail clip (attached to the switch)
- One RS-232 DB-9 to RJ-45 console cable
- CD User manual x 1
- Quick Installation Guide (QIG)

If any of the above items is missing or damaged, please contact your local sales representative.

2 Hardware Installation

This chapter includes hardware introduction, installation and configuration information.

Following topics are covered in this chapter:

2.1Hardware Introduction

Dimension

Panel Layout

Bottom View

Rear Side

2.2Wiring Power Inputs

2.3Wiring the Relay Output (DO)

2.4Wiring the Digital Input (DI)

2.5Connecting the Surge/ Lighting Protection

2.6Wiring Ethernet Ports

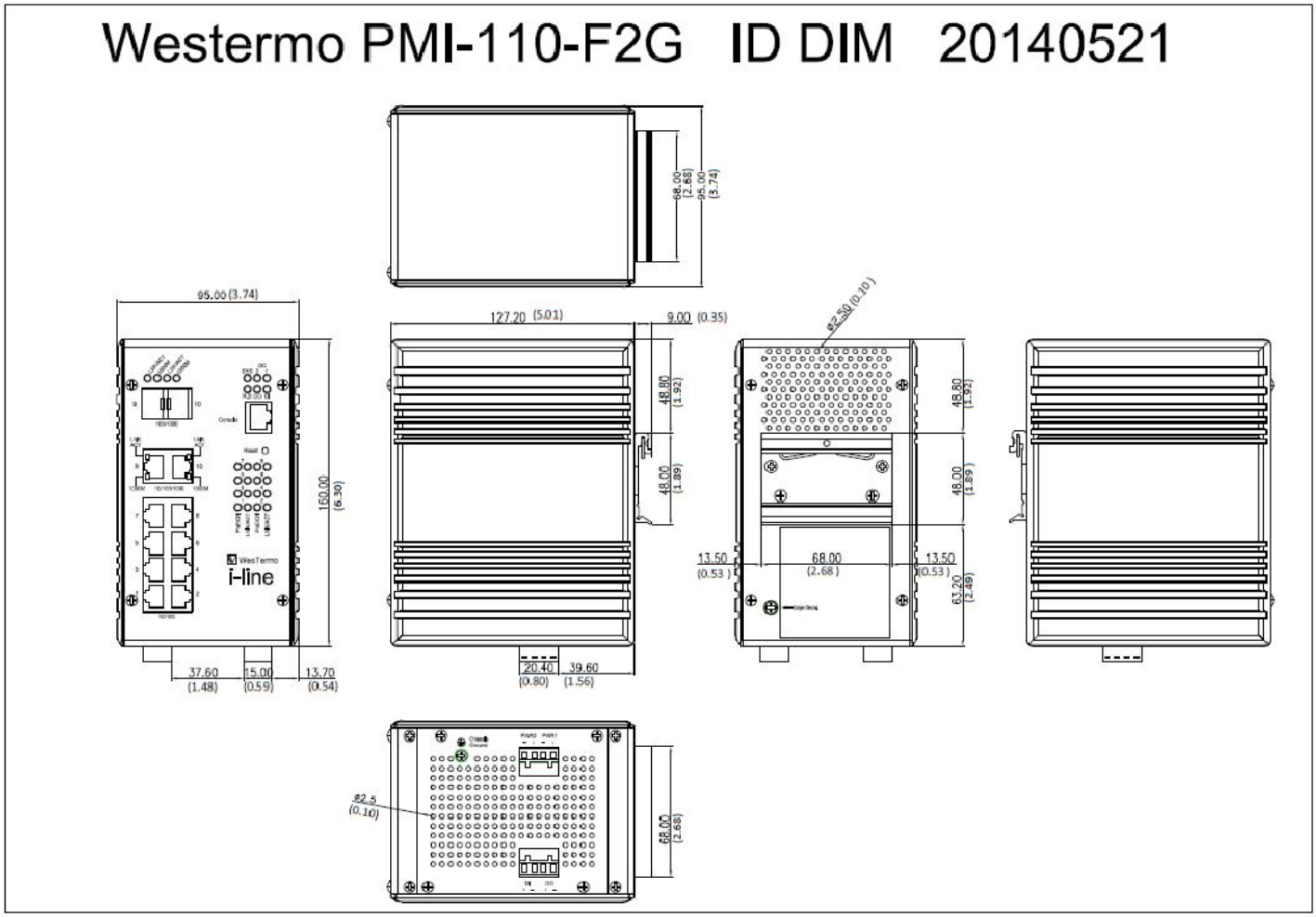
2.7Wall-mounting Installation

2.1 Hardware Introduction

Dimension –

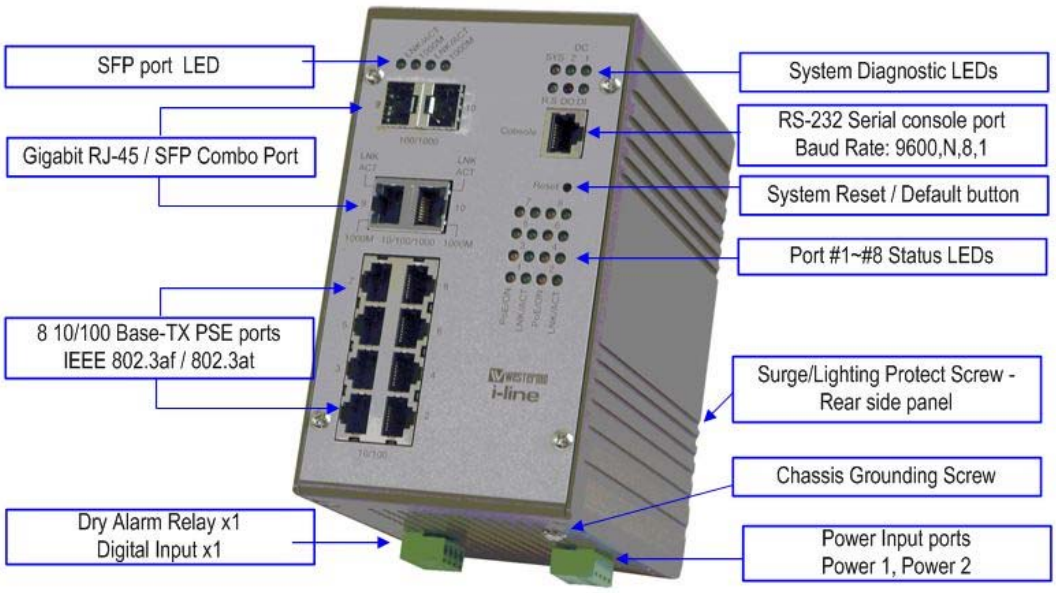
PMI-110-F2G w/o DIN Rail mounting kit: 95(W) x 127 (D)x 160(H)

PMI-110-F2G w/ DIN Rail mounting kit: 95(W) x 136.2 (D)x 160(H)



Panel Layout

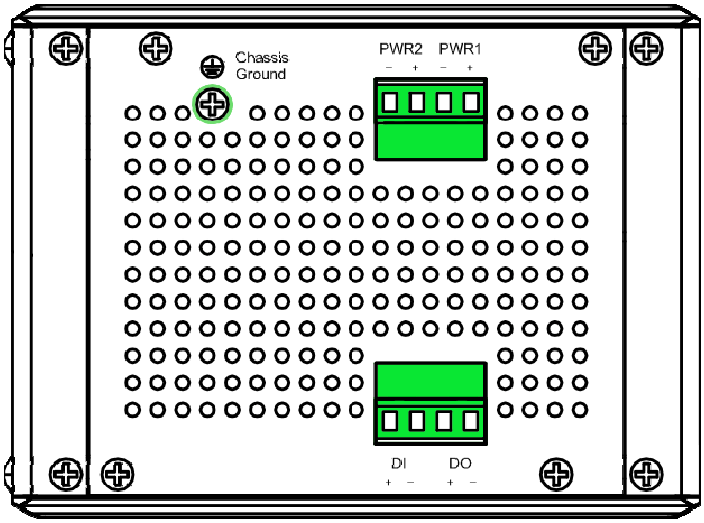
The front panel includes 8 x 10/100Mbps RJ-45 PoE ports, 2 x Gigabit Ethernet RJ-45/SFP socket ports, 1 RJ-45 for RS232 console, System diagnostic LEDs, Port LEDs, PoE status LEDs.



PMI-110-F2G Appearance

Bottom view

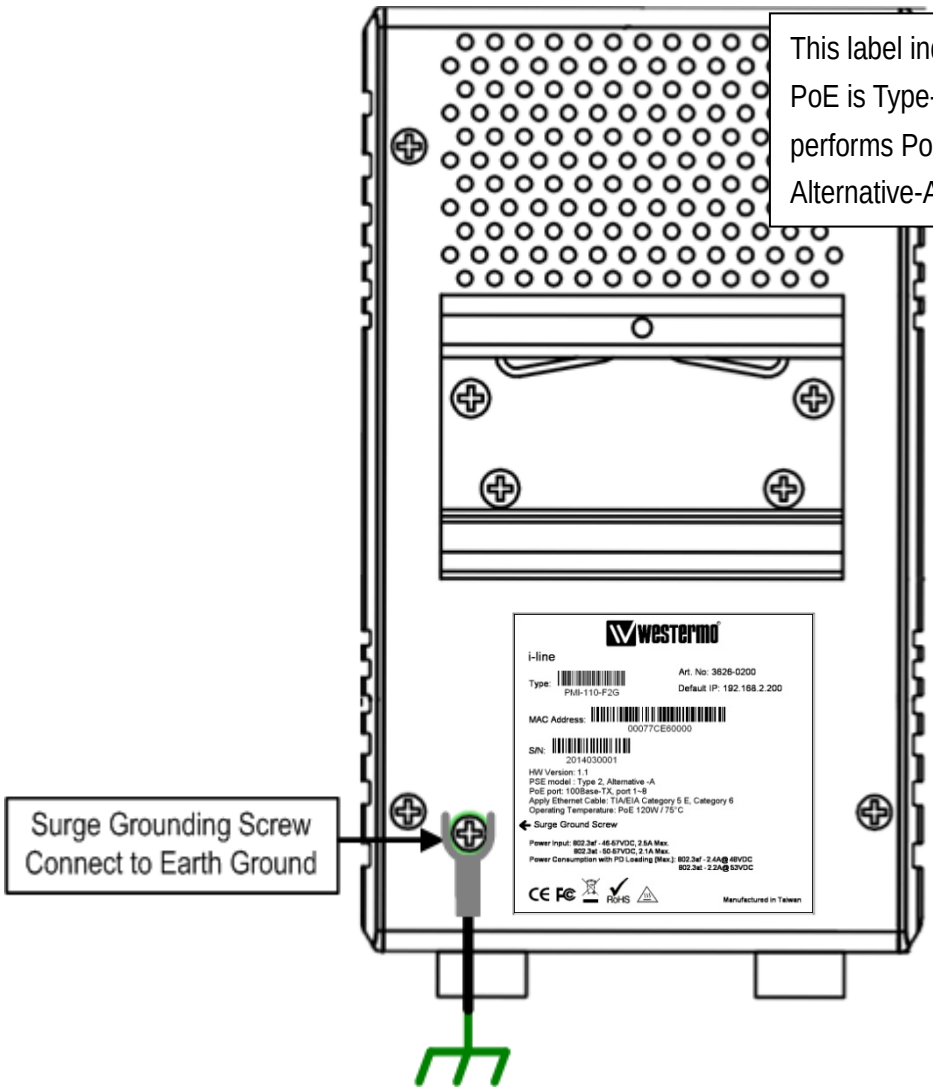
The bottom side includes 2 4-pin terminal block connectors and 1 chassis grounding screw. One of 4-pin terminal block connectors is for power inputs, and the rest is for alarm relay output and digital input.



Rear Side

The rear side back panel attached DIN rail clip and one lighting screw to make connection with chassis ground and Switch inner lighting protection circuit.

The product label is also sticked on the bottom side of DIN rail clip, in case if it is missed, please contact with your sales representive for product change.


This label indicates that the type of PoE is Type-2 high power PSE and performs PoE powering by Alternative-A mode (1,2,3,6)
Surge Grounding Screw
Connect to Earth Ground
i-line
Type: PMI-110-F2G
Art. No: 3626-0200
Default IP: 192.168.2.200
MAC Address: 00077CE60000
S/N: 2014030001
HW Version: 1.1
PSE model : Type 2, Alternative -A
PoE port: 100Base-TX, port 1~8
Apply Ethernet Cable: TIA/EIA Category 5 E, Category 6
Operating Temperature: PoE 120W / 75°C
Surge Ground Screw
Power Input: 802.3af - 46-57VDC, 2.5A Max.
802.3at - 50-57VDC, 2.1A Max.
Power Consumption with PD Loading (Max.): 802.3af - 2.4A@48VDC
802.3at - 2.2A@53VDC
Manufactured in Taiwan

2.2 Wiring Power Inputs

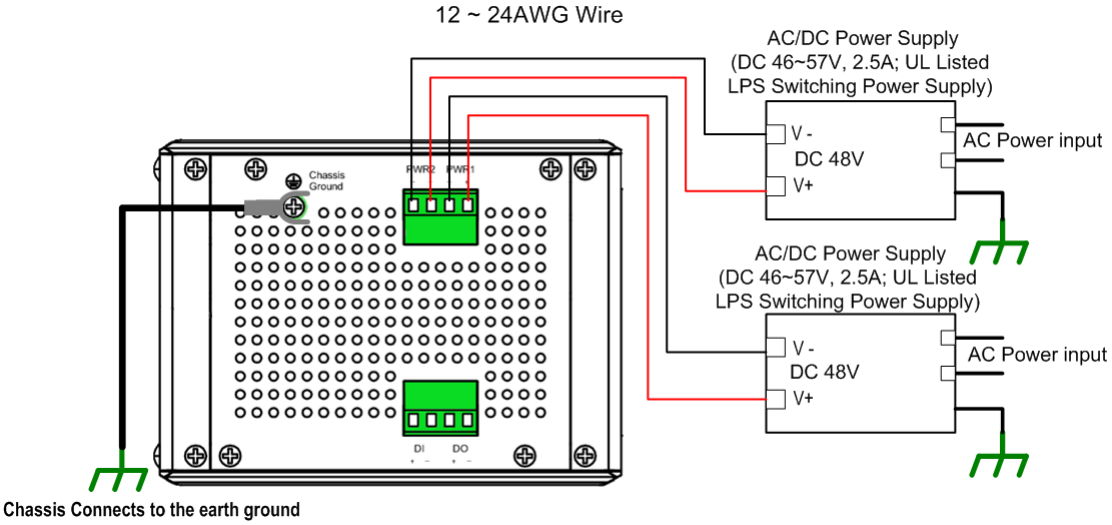
The Power input port is located at the bottom side, and provides 2 power input connections in one 4-pin removable terminal block. The power port support polarity reverse protection; the Switch won't start if wrong polarity applied. The wiring architecture please refers to below figure.

Wiring the Power Inputs

1. Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.
2. Tighten the wire-clamp screws to prevent the power wires from being loosened.
3. Connect the power wires to suitable AC/DC Switching type power supply. The PMI-110-F2G provides Power over Ethernet function and is compliant with IEEE802.3af/ IEEE802.3at standards; therefore, the input DC voltage should be in the range of DC 46V to DC 57V.

For the safety issue, turn off AC power input source before connecting the AC/DC Power supply module and the terminal block connectors. Besides, don't turn-on the source of AC/DC power module and make sure all connections were well done then power on the AC source to powering the Switch device. Otherwise, your screwdriver blade may inadvertently short your terminal connections to the grounded enclosure and cause damage.

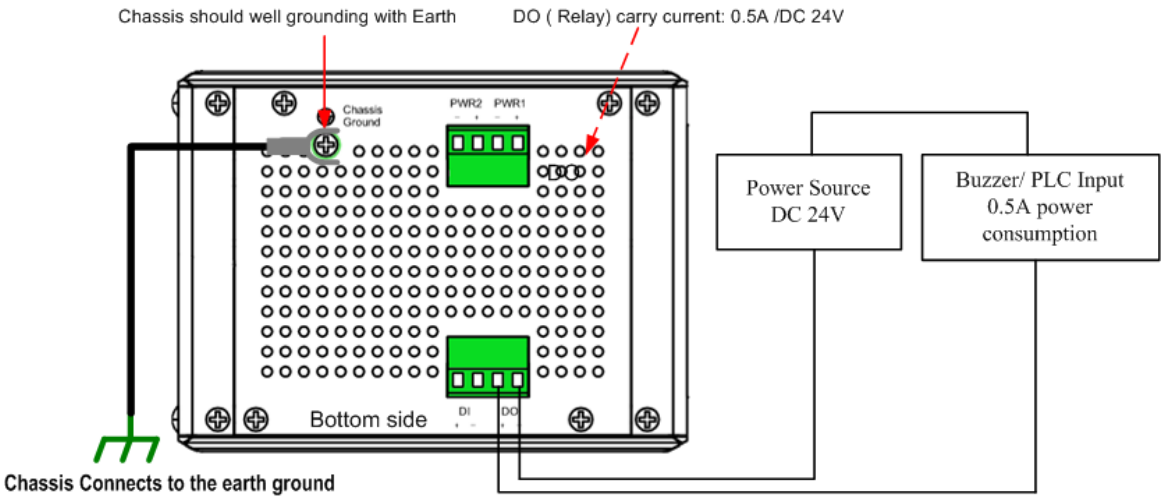
Notes: Use the **UL Listed LPS Power supply** with output Rating 46~57V Vdc, minimum 2.5A currents. Here, we recommended using DC 48V as the operating voltage. It is recommended to use 48vdc power supply.



Chassis Connects to the earth ground

2.3 Wiring the Relay Output (DO)

The relay output contacts are in the bottom side as shown on below figure. The relay output (DO) is controlled by the pre-defined operating rules. To activate relay output function, please refer to the CD User's Manual for more Relay Output management information.

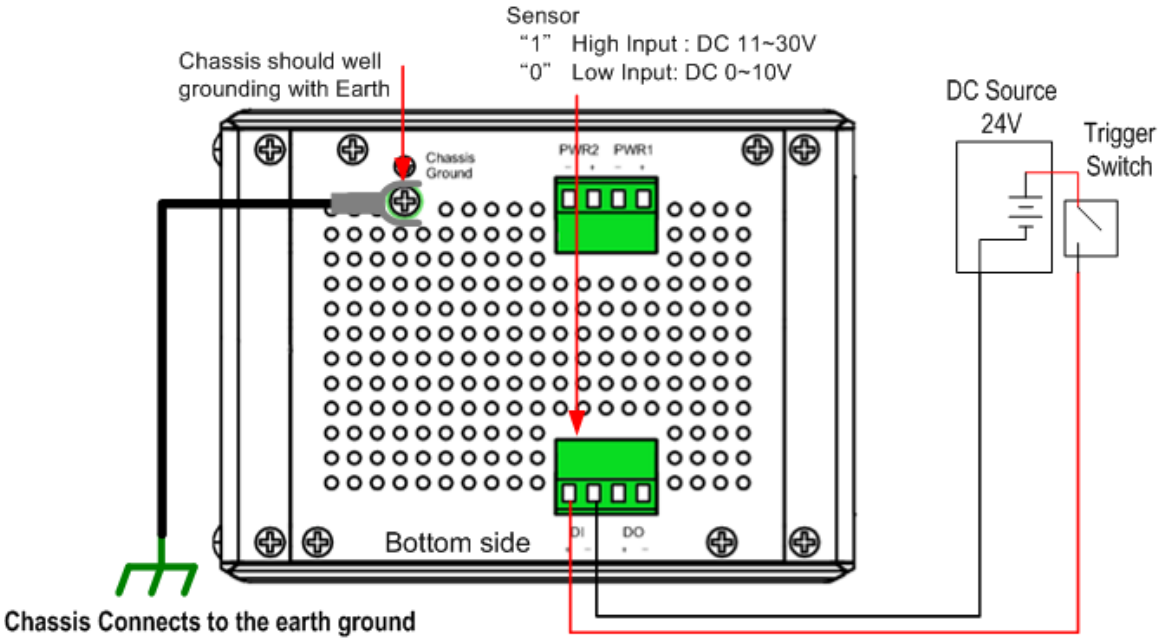


Digital Output Wiring simulate Diagram

Note: The relay contact only supports 0.5 A current, DC 24V. It is not recommended to apply voltage and current higher than the specifications.

2.4 Wiring the Digital Input (DI)

The Digital Input (D.I.) contacts are in the bottom side of the device as shown in below figure.
It accepts one external DC type signal input and can be configured to send alert message through Ethernet when the signal is changed. The signal may trigger and generated by external power switch, like as door open trigger switch for control cabinet.

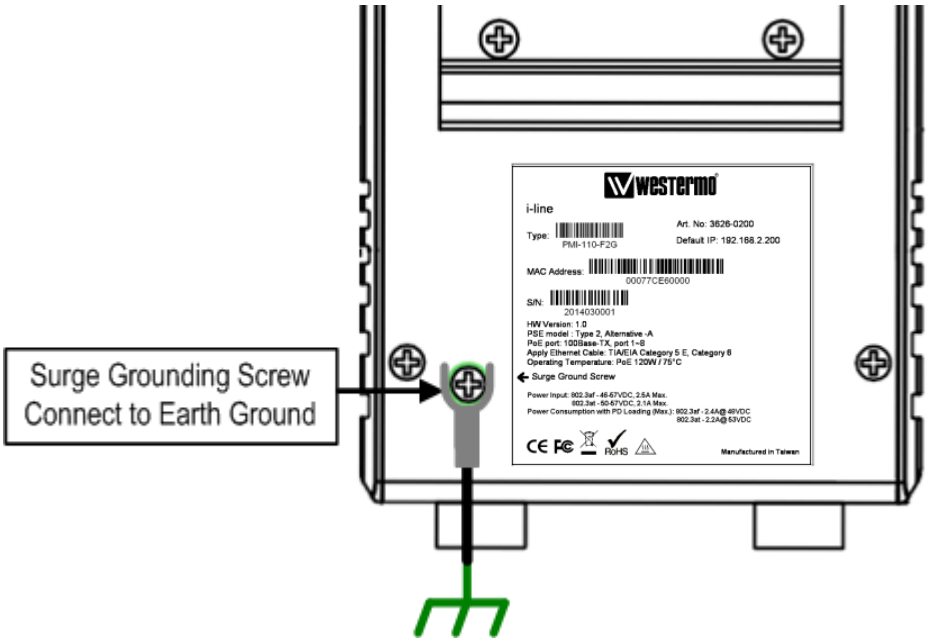


Digital Inputt Wiring simulate Diagram

Note: the DI accepts DC type signal and supports isolated input circuit with Digital High Level input DC 11V~30V and Digital Low Level input DC 0V~10V. Do not apply voltage that higher than the specification; it may cause internal circuit damage or a wrong action of DI.

2.5 Connecting the Surge /Lighting protection

There is one screw fixed on the rear side for lighting /surge protection; tighten and wire to chassis grounding to obtain better surge/ lighting immunity. But, do remember remove the surge grounding screw before to insulation/Hi-pot testing. In case you do not, the protectors may damage during the testing, and the lighting protection will malfunction.



Note: 1. Ensure the Surge/Lighting is well connecting with Chassis Grounding
2. Remove the Surge /Lighting Screw, before performing Insulation / Hi-pot Testing.

Never install or work on/with the equipment or the cabling during the period of its lightning activity.

2.6 Wiring Fast Ethernet PoE Ports

The PMI PoE Switch support 8 10/100Mbps Fast Ethernet ports with power over Ethernet (PoE) PSE function, and 2 Gigabit 10/100/1000Mbps RJ-45/SFP combo ports. Both of Gigabit combo ports provide SFP transceiver plug-in with first priority function.

Fast Ethernet Ports

The Fast Ethenert ports (1~8) comply with IEEE 802.3af / IEEE802.3at function with 120watts system power budget control function (enabled from firmware v1.2a); the PoE ports support alternative-A type powering method, and forward power through the RJ-45 conductors 1, 2, 3 and 6. If the power device (PD) is not fully compliant with IEEE 802.3af / IEEE 802.3at, then it will not be powering. So, before connecting the PD device, please ensure the PD you have bought is compliant with PoE standard. The RJ-45 plug's

conductor pin assignment shows as following table for your reference.

RJ-45 conductor	Type of Signal	Polarity of power	Note
1	RxD +	V -	Alternative-A
2	RxD -	V -	Alternative-A
3	TxD +	V+	Alternative-A
6	TxD -	V+	Alternative-A

Note: The PD device should accept power from either 1,2,3,6 (data pairs) or 4,5,7,8 (spare pairs); for the detail information, please refer to IEEE 802.3at / IEEE 802.3af Power over Ethernet standard.

Gigabit Ethernet /SFP combo port

The PMI-110-F2G provides 2 Gigabit RJ-45/ SFP combo ports that with different link speed – 10Mbps, 100Mbps, 1000Mbps, and compliant with the standards of IEEE 802.3 10Base-T, IEEE 82.3u 100Base-TX, IEEE 8023.u 100Base-FX, IEEE 802.3ab 1000Base-T, and IEEE 802.3z Gigabit fiber.

The combo ports support SFP transceiver plug-in high priority function; thus, don't connect Ethernet RJ-45 and insert SFP transceiver at the same time; it will cause the port being activated in wrong status.

The SFP ports also provide Digital Diagnostic Monitoring function, it can assist user to monitor the quality of optical signal, and diagnose the transmission of fiber. This function is only available for Westermo recomended DDM SFP transceiver, and does not support third party transceiver that may not fully comply with MSA SFP transceiver standard.

By the DDM function, user can get real information including the strength of received optical signal, launched optical signal and current operating temperature of SFP transceiver, and the specification of transceiver.

The following diagram shows the information captured from WEB user interface.

SFP DDM

Port	SFP Scan / Eject	SFP DDM	Temperature (°C)		Tx Power (dBm)		Rx Power (dBm)	
			Current	Range	Current	Range	Current	Range
9	Scan	Disable	--	--	--	--	--	--
10	Scan	Disable	--	--	--	--	--	--

Range: the specification of Westermo defined.

Current: actual value read from SFP transceiver.

Tx Power (dBm): optical strength of received.

Rx Power (dBm): optical strength of launched.

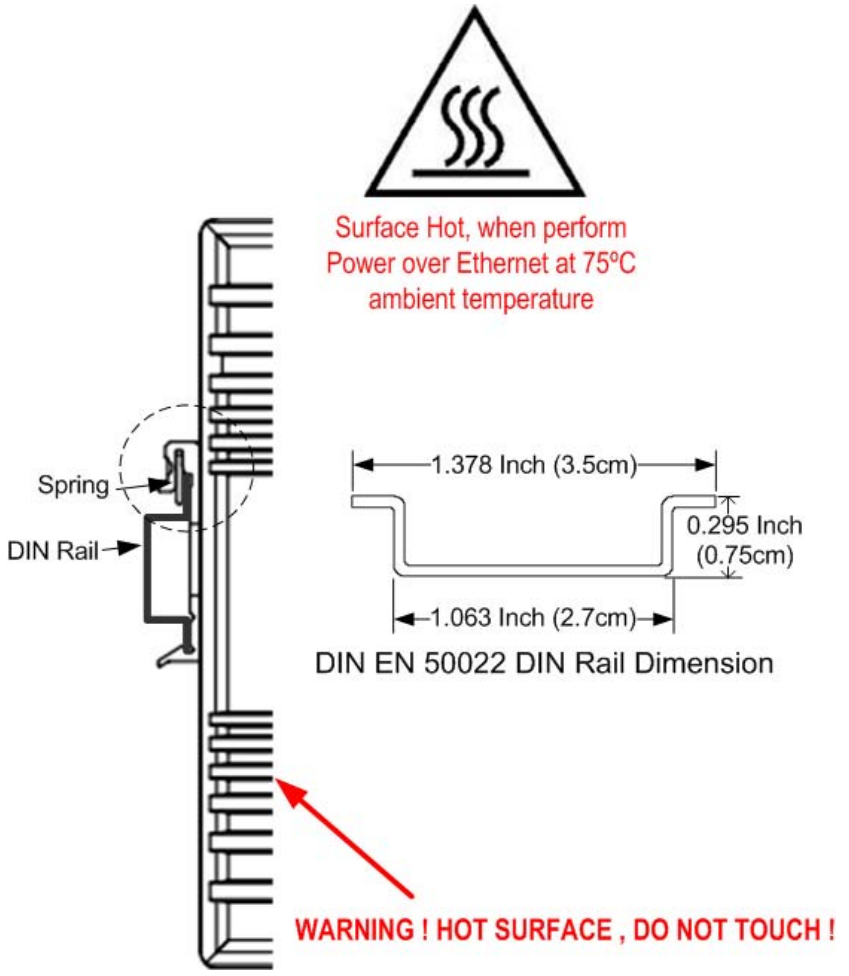
Note: The Ethernet Switch has to use UL recognized fiber transceiver with Class 1 Laser/LED Diode.

Note: It is recommended to not plug-in SFP fiber transceiver and link up RJ-45 port at the same time, it might cause the connection does not working properly.

2.7 DIN Rail mounting Installation

The DIN-Rail clip is already screwed tight on the rear side of PMI Switch when shipping. If the DIN-Rail clip is not screwed on the rear side panel, please contact your distributor to get the DIN rail clip set. The DIN rail clip supports EN50022 standard. The diagram following includes the dimension of EN50022 DIN rail for your reference.

The Switch should install and used at Restriced Acess Location area, like as the control room or control cabinet. Besides, the device's surface temperature may caused damage while the Power over Ethernet function is enabled and under working, at the ambient temperature 70°C . Therefore, the device should install at the restriced location, like as Control cabinet to prevent any damage.



Follow the steps below to mount PMI Managed Switch to the DIN-Rail track:

1. First, insert the DIN-Rail track upper side into the upper end of DIN-Rail clip.
2. Lightly push the bottom of DIN-Rail clip into the track.
3. Check if DIN-Rail clip is tightly attached to the EN50022 Rail track.
4. To remove PMI Switch from the track, reverse the steps above.

Notes: 1. The DIN Rail should compliant with DIN EN50022 standard. Using wrong DIN rail may cause unsafe installation.

2. For UL Safety consideration- the equipment is designed for in building installation only and is not intended to be connected to exposed (outside plant) networks.

3 Preparation for Management

PMI Industrial Managed PoE Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose network connection to your PMI PoE Managed Switch. This is so-called out-band management. It wouldn't be affected by network performance.

The in-band management means you can remotely manage the switch via the network. You can choose Telnet or Web-based management. You just need to know the device's IP address and you can remotely connect to its embedded HTTP web pages or Telnet console.

Following topics are covered in this chapter:

3.1Preparation for Serial Console

3.2Preparation for Web Interface

3.3Preparation for Telnet console

3.1 Preparation for Serial Console

In the unit package, Westermo attached one RJ-45 to RS-232 DB-9 console cable. Please attach RS-232 DB-9 connector to your PC's COM port, connect RJ-45 connector to the Console port of the PMI PoE Managed Switch. If the serial cable is lost, please follow the serial console cable PIN assignment to find one. (Refer to the appendix).

1. Go to Start -> Program -> Accessories -> Communication -> Hyper Terminal
2. Give a name to the new console connection.
3. Choose the COM name
4. Select correct serial settings. The serial settings of PMI PoE Managed Switches are as below:

   Baud Rate: 9600 / Parity: None / Data Bit: 8 / Stop Bit: 1

5. After connected, you can see Switch login request.
6. Login the switch. The default username is "admin", password, "westermo".

```
Switch login: admin
Password:

The switch (version 1.1.5-20100414-11:04:13).

Switch>
```

3.2 Preparation for Web Interface

PMI Managed PoE Switch provides HTTP Web Interface and Secured HTTPS Web Interface for web management.

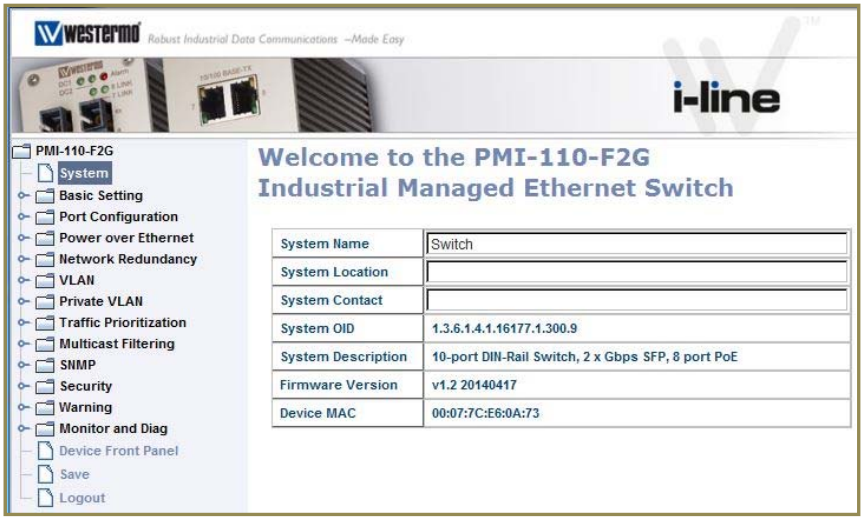
3.2.1 Web Interface

Westermo web management page is developed by JAVA. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla, to configure and interrogate the switch from anywhere on the network.

Before you attempt to use the embedded web interface to manage switch operation, verify that your PMI Managed PoE Switch is properly installed on your network and that every PC on this network can access the switch via the web browser.

1. Verify that your network interface card (NIC) is operational, and that your operating system supports TCP/IP protocol.
2. Wire DC power to the switch and connect your switch to your computer.
3. Make sure that the switch default IP address is 192.168.2.200.
4. Change your computer IP address to 192.168.2.2 or other IP address which is located in the 192.168.2.x (Network Mask: 255.255.255.0) subnet.
5. Switch to DOS command mode and ping 192.168.2.200 to verify a normal response time.
   Launch the web browser and Login.
6. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
7. Type **http://192.168.2.200** (or the IP address of the switch). And then press **Enter**.
8. The login screen will appear next.
9. Key in user name and the password. Default user name is **admin** and password **westermo**.

Click on **Enter** or **OK**. The Welcome page of the web-based management interface will then appear.



Once you enter the web-based management interface, you can freely change the PMI's IP address to fit your network environment.

Note 1: IE 5.0 or later versions do not allow Java applets to open sockets by default. Users have to directly modify the browser settings to selectively enable Java applets to use network ports.

Note 2: The Web UI connection session of PMI managed Switch will be logged out automatically if you don't give any input after 30 seconds. After logged out, you should re-login and key in correct user name and password again.

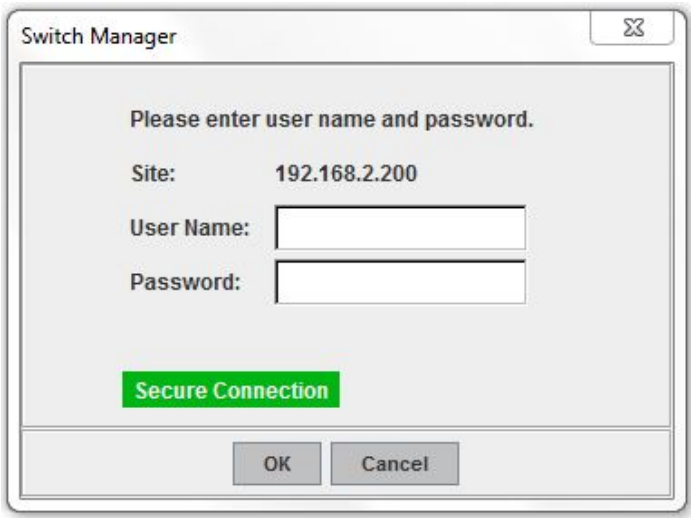
3.2.2 Secured Web Interface

Westermo web management page also provides secured management HTTPS login. All the configuration commands will be secured and will be hard for the hackers to sniff the login password and configuration commands.

Launch the web browser and Login.

1. Launch the web browser (Internet Explorer or Mozilla Firefox) on the PC.
2. Type **https://192.168.2.200** (or the IP address of the switch). And then press **Enter**.
3. The popup screen will appear and request you to trust the secured HTTPS connection distributed by PMI PoE Managed Switch first. Click "**Yes"** to trust it.

4. The login screen will appear next.



5. Key in the user name and the password. Default user name is **admin** and password **westermo**.
6. Click on **Enter** or **OK.** Welcome page of the web-based management interface will then appear.
7. Once you enter the web-based management interface, all the commands you see are the same as what you see by HTTP login.

3.3 Preparation for Telnet Console

3.3.1 Telnet

Westermo PMI managed Switch supports Telnet console. You can connect to the switch by Telnet and the command lines are the same as what you see by RS232 console port. Below are the steps to open Telnet connection to the switch.

1. Go to Start -> Run -> cmd. And then press **Enter**
2. Type the **Telnet 192.168.2.200** (or the IP address of the switch). And then press **Enter**

3.3.2 SSH (Secure Shell)

Westermo PMI managed Switch also support SSH console. You can remotely connect to the switch by command line interface. The SSH connection can secure all the configuration commands you sent to the switch.

SSH is a client/server architecture while the Switch is the SSH server. When you want to make SSH connection with the switch, you should download the SSH client tool first.

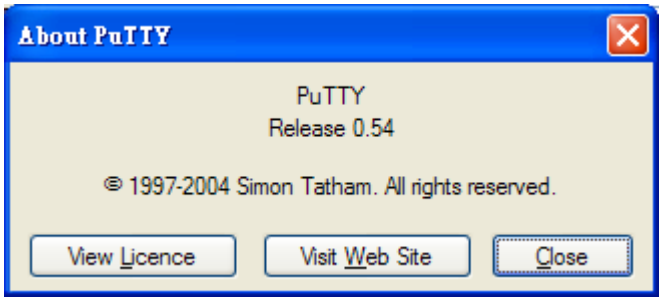
SSH Client

There are many free, sharewares, trials or charged SSH clients you can find on the internet. Fox example, PuTTY is a free and popular Telnet/SSH client.

We'll use this tool to demonstrate how to login PMI by SSH. Note: *PuTTY is copyright 1997-2006 Simon Tatham*.

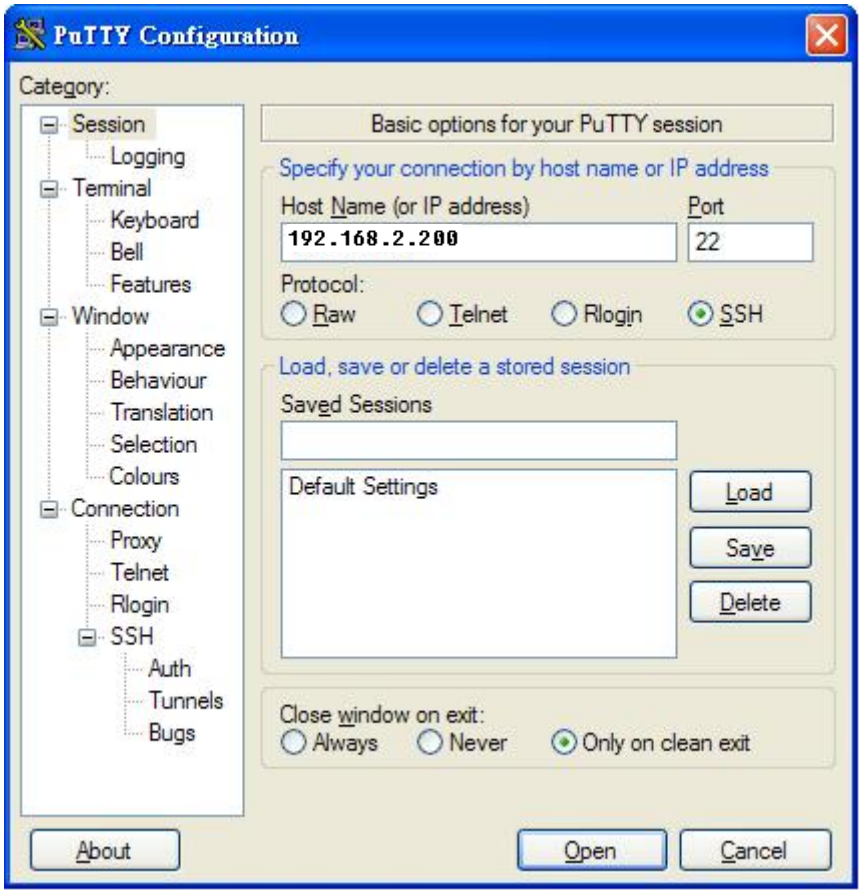
Download
PuTTY: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

The copyright of **PuTTY**



1. Open SSH Client/PuTTY

In the **Session** configuration, enter the **Host Name** (IP Address of your PMI switch) and **Port number** (default = 22). Choose the "**SSH**" protocol. Then click on "**Open**" to start the SSH session console.



2. After click on **Open**, then you can see the cipher information in the popup screen. Press **Yes** to accept the Security Alert.

PuTTY Security Alert
The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 55:cf:c9:67:12:d6:3f:f4:30:6c:f8:50:c0:6e:41:3d
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.
Yes(Y)
No(N)
Cancel

3. After few seconds, the SSH connection to Switch is opened.
4. Type the Login Name and its Password. The default Login Name and Password are **admin / westermo**.
5. All the commands you see in SSH are the same as the CLI commands you see via RS232 console. The next chapter will introduce in detail how to use command line to configure the switch.

4 Feature Configuration

This chapter explains how to configure PMI Managed software features. There are four ways to access the switch: Serial console, Telnet, Web browser and SNMP.

PMI Managed Switch provides both in-band and out-band configuration methods. You can configure the switch via RS232 console cable if you don't attach your admin PC to your network, or if you lose the network connection to your PMI switch. This is so-called out-band management. It wouldn't be affected by the network performance.

The in-band management means you can remotely manage the switch via the network. You can choose Telnet or Web-based management. You just need to know the device's IP address. Then you can remotely connect to its embedded HTML web pages or Telnet console.

Westermo web management page is developed by Java. It allows you to use a standard web-browser such as Microsoft Internet Explorer, or Mozilla, to configure and interrogate the switch from anywhere on the network.

Note: IE 5.0 or later versions do not allow Java applets to open sockets by default. Users have to directly modify the browser settings to selectively enable Java applets to use network ports.

Following topics are covered in this chapter:

4.1 Command Line Interface (CLI) Introduction
4.2 Basic Setting
4.3 Port Configuration
4.4 Power over Ethernet
4.5 Network Redundancy
4.6 VLAN
4.7 Private VLAN
4.8 Traffic Prioritization
4.9 Multicast Filtering
4.10 SNMP
4.11 Security
4.12 Warning
4.13 Monitor and Diag
4.14 Device Front Panel
4.15 Save
4.16 Logout

4.1 Command Line Interface Introduction

The Command Line Interface (CLI) is the user interface to the switch's embedded software system. You can view the system information, show the status, configure the switch and receive a response back from the system by keying in a command.

There are some different command modes. Each command mode has its own access ability, available command lines and uses different command lines to enter and exit. These modes are User EXEC, Privileged EXEC, Global Configuration, (Port/VLAN) Interface Configuration modes.

User EXEC mode: As long as you login the switch by CLI. You are in the User EXEC mode. You can ping, telnet remote device, and show some basic information.

Type **enable** to enter next mode, **exit** to logout. **?** to see the command list

```
Switch>
  enable      Turn on privileged mode command
  exit        Exit current mode and down to previous mode
  list        Print command list
  ping        Send echo messages
  quit        Exit current mode and down to previous mode
  show        Show running system information
  telnet      Open a telnet connection
  traceroute  Trace route to destination
```

Privileged EXEC mode: Press enable in the User EXEC mode, then you can enter the Privileged EXEC mode. In this mode, the system allows you to view current configuration, reset default, reload switch, show system information, save configuration…and enter the global configuration mode.

Type **configure terminal** to enter next mode, **exit** to leave. **?** to see the command list

```
Switch#
  archive        Manage archive files
  clear          Reset functions
  clock          Configure time-of-day clock
  configure      Configuration from vty interface
  copy           Copy from one file to another
  debug          Debugging functions (see also 'undebug')
  disable        Turn off privileged mode command
  dot1x          IEEE 802.1x standard access security control
  end            End current mode and change to enable mode
  exit           Exit current mode and down to previous mode
  hardware       hardware function
  list           Print command list
  no             Negate a command or set its defaults
  pager          Terminal pager
  ping           Send echo messages
  quit           Exit current mode and down to previous mode
  reboot         Reboot system
  reload         copy a default-config file to replace the current one
  show           Show running system information
  telnet         Open a telnet connection
  terminal       Set terminal line parameters
  traceroute     Trace route to destination
  write          Write running configuration to memory, network, or terminal
```

Global Configuration Mode: Press **configure terminal** in privileged EXEC mode. You can then enter global configuration mode. In global configuration mode, you can configure all the features that the system provides you.

Type **interface IFNAME/VLAN** to enter interface configuration mode, **exit** to leave. **?** to see the command list.

Available command lists of global configuration mode.

```
Switch(config)#
  administrator          Administrator account setting
  arp                    Set a static ARP entry
  clock                  Configure time-of-day clock
  default                Set a command to its defaults
  dot1x                  IEEE 802.1x standard access security control
  end                    End current mode and change to enable mode
  ethertype              Ethertype
  exit                   Exit current mode and down to previous mode
  gmrp                   GMRP protocol
  gvrp                   GARP VLAN Registration Protocol
  hostname               Set system's network name
  interface              Select an interface to configure
  ip                     IP information
  lacp                   Link Aggregation Control Protocol
  list                   Print command list
  lldp                   Link Layer Discovery Protocol
  log                    Logging control
  mac-address-table      mac address table
  mirror                 Port mirroring
  modbus                 Modbus TCP Slave
  multiple-super-ring    Configure Multiple Super Ring
  nameserver             DNS Server
  no                     Negate a command or set its defaults
  ntp                    Configure NTP
  poe                    Configure power over ethernet
  ptpd                   IEEE1588 Precision Time Protocol
  qos                    Quality of Service (QoS)
  relay                  relay output type information
  router                 Enable a routing process
  sfp                    Small form-factor pluggable
  smtp-server            SMTP server configuration
  snmp-server            the SNMP server
  spanning-tree          the spanning tree algorithm
  trunk                  Trunk group configuration
  vlan                   Virtual LAN
  warning-event          Warning event selection
  write-config           Specify config files to write to
Switch(config)#
```

(Port) Interface Configuration: Press **interface IFNAME** in global configuration

mode. You can then enter interface configuration mode. In this mode, you can configure port settings.

The port interface name for fast Ethernet port 1 is fa1,… fast Ethernet 7 is fa7, fast Ethernet port 8 is fa8.. Gigabit Ethernet port 9 is gi9 and port 10 is gi10. Type the interface name accordingly when you want to enter certain interface configuration mode.

Type "**exit"** to leave current level.

Type "**?"** to see the command list

Available command lists of the global configuration mode.

```
Switch(config)# interface fa1
Switch(config-if)#

acceptable          Configures the 802.1Q acceptable frame types of a port.
  auto-negotiation  Enables auto-negotiation state of a given port
  description       Interface specific description
  dot1x             IEEE 802.1x standard access security control
  duplex            Specifies the duplex mode of operation for a port
  end               End current mode and change to enable mode
  exit              Exit current mode and down to previous mode
  flowcontrol       Sets the flow-control value for an interface
  garp              General Attribute Registration Protocol
  ingress           802.1Q ingress filtering features
  lacp              Link Aggregation Control Protocol
  list              Print command list
  loopback          Specifies the loopback mode of operation for a port
  mdix              Configure mdix state of a given port
  mtu               Specifies the MTU on a port.
  no                Negate a command or set its defaults
  poe               Configure power over ethernet
  qos               Quality of Service (QoS)
  quit              Exit current mode and down to previous mode
  rate-limit        Rate limit configuration
  sfp               Small form,-factor pluggable
  shutdown          Shutdown the selected interface
  spanning-tree     the spanning-tree protocol
  speed             Specifies the speed of a Fast Ethernet port or a Gigabit
                    Ethernet port.
  switchport        Set switching mode characteristics
```

(VLAN) Interface Configuration: Press **interface VLAN VLAN-ID** in global configuration mode. You can then enter VLAN interface configuration mode. In this mode, you can configure the settings for the specific VLAN.

The VLAN interface name of VLAN 1 is VLAN 1, VLAN 2 is VLAN 2…

Type **exit** to leave the mode. Type **?** to see the available command list.

The command lists of the VLAN interface configuration mode.

```
Switch(config)# interface vlan 1
Switch(config-if)#
  description   Interface specific description
  end             End current mode and change to enable mode
  exit            Exit current mode and down to previous mode
  ip              Interface Internet Protocol config commands
  list            Print command list
  no              Negate a command or set its defaults
  quit            Exit current mode and down to previous mode
  shutdown        Shutdown the selected interface
```

Summary of the 5 command modes.

Command Mode	**Main Function**	**Enter and Exit Method**	**Prompt**
User EXEC	This is the first level of access. User can ping, telnet remote device, and show some basic information	Enter: **Login** successfully Exit: **exit** to logout. Next mode: Type **enable** to enter privileged EXEC mode.	Switch>
Privileged EXEC	In this mode, the system allows you to view current configuration, reset default, reload switch, show system information, save configuration…and enter global configuration mode.	Enter: Type **enable** in User EXEC mode. Exec: Type **disable** to exit to user EXEC mode. Type **exit** to logout Next Mode: Type **configure terminal** to enter global configuration command.	Switch#
Global configuration	In global configuration mode, you can configure all the features that the system provides you	Enter: Type **configure terminal** in privileged EXEC mode Exit: Type **exit** or **end** or press **Ctrl-Z** to exit. Next mode: Type **interface IFNAME/ VLAN VID** to enter interface configuration mode	Switch(config)#
Port Interface configuration	In this mode, you can configure port related settings.	Enter: Type **interface IFNAME** in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	Switch(config-if)#
VLAN Interface	In this mode, you can configure	Enter: Type **interface VLAN VID**	Switch(config-vlan)#

Configuration	settings for specific VLAN.	in global configuration mode. Exit: Type **exit** or **Ctrl+Z** to global configuration mode. Type **end** to privileged EXEC mode.	

Here are some useful commands for you to see these available commands. Save your time in typing and avoid typing error.

? To see all the available commands in this mode. It helps you to see the next command you can/should type as well.

```
Switch(config)# interface (?)
  IFNAME   Interface's name
  vlan     Select a vlan to configure
```

(Character)? To see all the available commands starts from this character.

```
Switch(config)# a?
  access-list      Add an access list entry
  administrator    Administrator account setting
  arp              Set a static ARP entry
```

The tab key helps you to input the command quicker. If there is only one available command in the next, clicking on tab key can help to finish typing soon.

```
Switch# co (tab) (tab)
Switch# configure terminal

Switch(config)# ac (tab)
Switch(config)# access-list
```

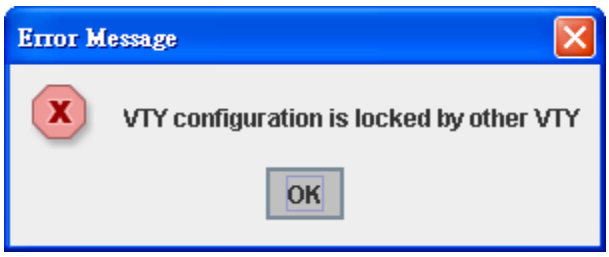
Ctrl+C To stop executing the unfinished command.

Ctrl+S To lock the screen of the terminal. You can't input any command.

Ctrl+Q To unlock the screen which is locked by Ctrl+S.

Ctrl+Z To exit configuration mode.

Alert message when multiple users want to configure the switch. If the administrator is in configuration mode, then the Web users can't change the settings. PMI Managed Switch allows only one administrator to configure the switch at a time.



4.2 Basic Setting

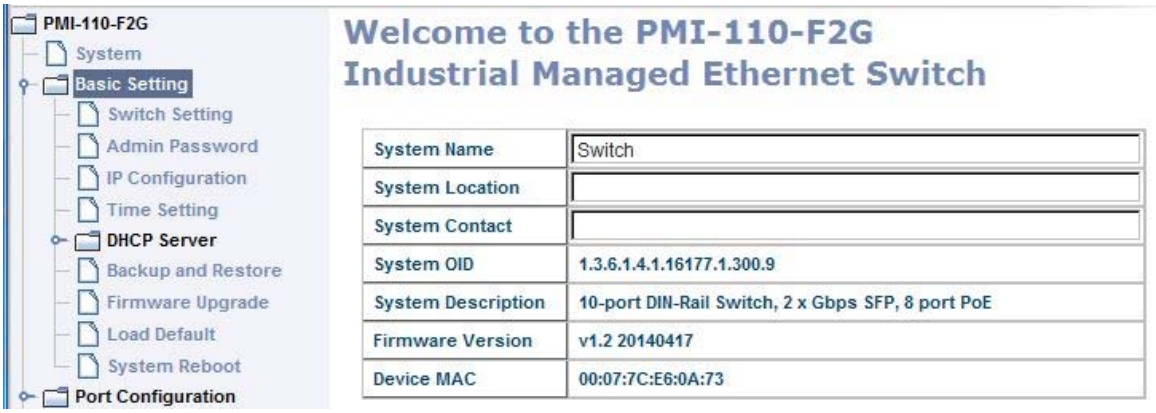
The Basic Setting group provides you to configure switch information, IP address and user name/Password of the system. It also allows you to do firmware upgrade, backup and restore configuration, reload factory default, and reboot the system.

Following commands are included in this group:

4.2.1 Switch Setting
4.2.2 Admin Password
4.2.3 IP Configuration
4.2.4 Time Setting
4.2.5 DHCP Server
4.2.6 Backup and Restore
4.2.7 Firmware Upgrade
4.2.8 Factory Default
4.2.9 System Reboot
4.2.10 CLI Commands for Basic Setting

4.2.1 Switch Basic Setting

You can assign System name, Location, Contact and view system information.



System Name: You can assign a name to the device. The available characters you can input is 64. After you configure the name, CLI system will select the first 12 characters as the name in CLI system.

System Location: You can specify the switch's physical location here. The available characters you can input are 64.

System Contact: You can specify contact people here. You can type the name, mail address or other information of the administrator. The available characters you can input are 64.

System OID: The SNMP object ID of the switch. You can follow the path to find its

private MIB in MIB browser. (**Note:** When you attempt to view private MIB, you should compile private MIB files into your MIB browser first.)

System Description: the name of this managed product.

Firmware Version: Display the firmware version installed in this device.

MAC Address: Display unique hardware address (MAC address) assigned by the manufacturer.

Once you finish the configuration, click on **Apply** to apply your settings.

Note: Always remember to select **Save** to save your settings. Otherwise, the settings you made will be lost when the switch is powered off.

4.2.2 Admin Password

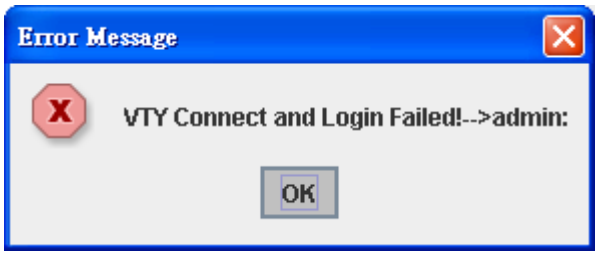
You can change the user name and the password here to enhance security

User name: You can key in new user name here. The default setting is **admin**.

Password: You can key in new password here. The default setting is **westermo**.

Confirm Password: You need to type the new password again to confirm it.

Once you finish configuring the settings, click on **Apply** to apply your configuration.



4.2.3 IP Configuration

This function allows users to configure the switch's IP address settings. Below figure is the UI of IP configuraation.

DHCP Client: You can select to **Enable** or **Disable** DHCP Client function. When DHCP Client function is enabled, an IP address will be assigned to the switch from the network's DHCP server. In this mode, the default IP address will therefore be replaced by the one assigned by DHCP server. If DHCP Client is disabled, then the IP address that you specified will be used instead.

IP Address: You can assign the IP address reserved by your network for your PMI. If DHCP Client function is enabled, you don't need to assign an IP address to the PMI, as it will be overwritten by DHCP server and shown here. The default IP is 192.168.2.200.

Subnet Mask: You can assign the subnet mask for the IP address here. If DHCP Client function is enabled, you don't need to assign the subnet mask. The default Subnet Mask is 255.255.255.0.

Note: In the CLI, we use the enabled bit of the subnet mask to represent the number displayed in web UI. For example, 8 stands for 255.0.0.0; 16 stands for 255.255.0.0; 24 stands for 255.255.255.0.

Default Gateway: You can assign the gateway for the switch here. **Note:** In CLI, we use 0.0.0.0/0 to represent for the default gateway.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

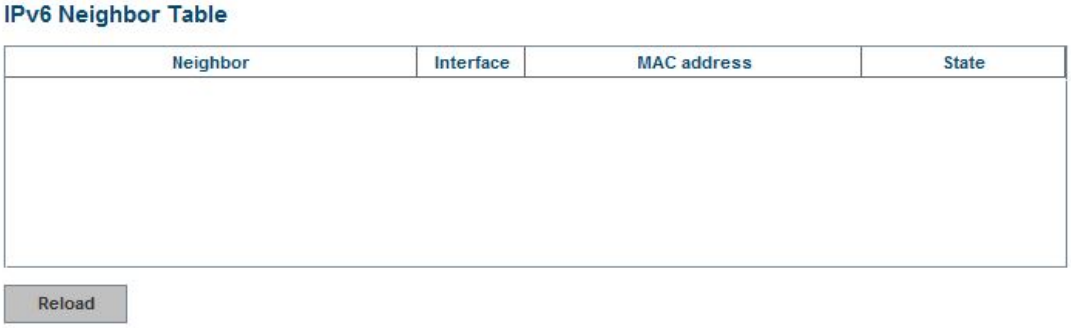
IPv6 Configuration –An IPv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (:), and the length of IPv6 address is 128bits.

An example of an IPv6 address is: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

The default IP address of MRI-128-F4G Managed Switch is assigned from MAC

address, for example fe80:0:0:0:207:7cff:fee6:00, and the Leading zeroes in a group may be omitted. Thus, the example address may be written as: fe80::207:7cff:fe60:0.

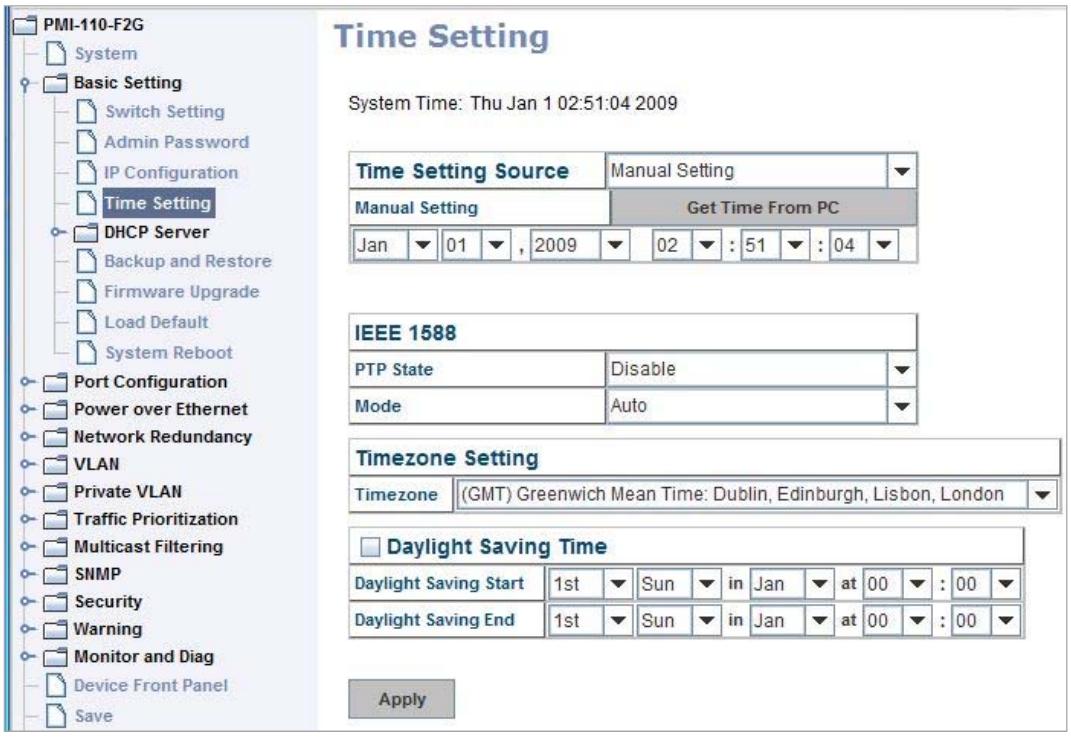
IPv6 Address field: typing new IPv6 address in this field.
Prefix: the size of subnet or netwok, and it equivalent to the subnetmask, but written in different. The default subnet mask length is 64bits, and writen in decimal value - 64.
Add: after add new IPv6 address and prefix, don't forget click icon -"**Add**" to apply new address to system.
Remove: select existed IPv6 address and click icon -"**Remove**" to delete IP address.
Reload: refresh and reload IPv6 address listing.
IPv6 Neighbor Table: shows the IPv6 address of neighbor, connected interface, MAC address of remote IPv6 device, and current state of neighbor device.



The system will update IPv6 Neighbor Table automatically, and user also can click the icon "**Reload**" to refresh the table.

4.2.4 Time Setting

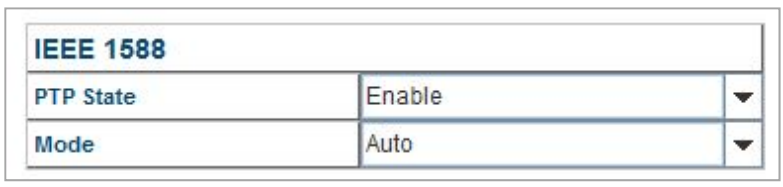
Time Setting source allow user to set the time manually or through NTP server. Network Time Protocol (NTP) is used to synchronize computer clocks on the internet. You can configure NTP settings here to synchronize the clocks of several switches on the network. Below figure is similar as PMI Switch.



Manual Setting: User can select Manual setting to change time as user wants. User also can click the button “Get Time from PC” to get PC’s time setting for switch.

NTP client: Select the Time Setting Source to NTP client can let device enable the NTP client service. NTP client will be automatically enabled if you change Time source to NTP Client. The system will send request packet to acquire current time from the NTP server you assigned.

IEEE 1588: With the **Precision Time Protocol IEEE 1588** there is now, for the first time, a standard available which makes it possible to synchronize the clocks of different end devices over a network at speeds faster than one Micro-second.



To enable IEEE 1588, select Enable in PTP Status and choose Auto, Master or Slave Mode. After time synchronized, the system time will display the correct time of the PTP server.

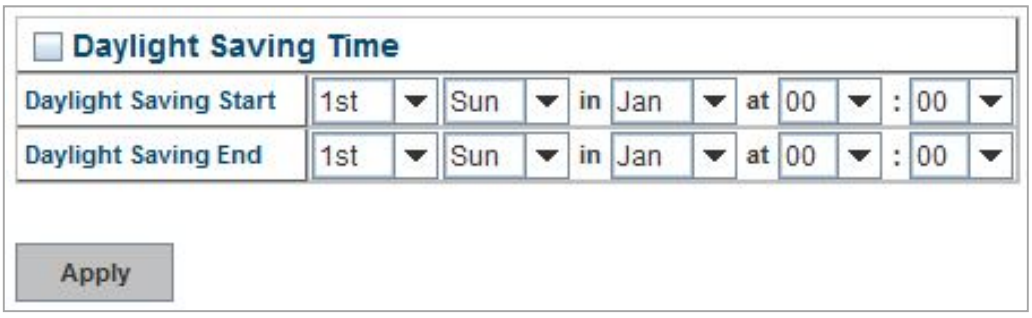
Time-zone: Select the time zone where the switch is located. Following table lists the time zones for different locations for your reference. The default time zone is GMT Greenwich Mean Time.

Switch(config)# clock timezone

01 (GMT-12:00) Eniwetok, Kwajalein
02 (GMT-11:00) Midway Island, Samoa
03 (GMT-10:00) Hawaii
04 (GMT-09:00) Alaska
05 (GMT-08:00) Pacific Time (US & Canada) , Tijuana
06 (GMT-07:00) Arizona
07 (GMT-07:00) Mountain Time (US & Canada)
08 (GMT-06:00) Central America
09 (GMT-06:00) Central Time (US & Canada)
10 (GMT-06:00) Mexico City
11 (GMT-06:00) Saskatchewan
12 (GMT-05:00) Bogota, Lima, Quito
13 (GMT-05:00) Eastern Time (US & Canada)
14 (GMT-05:00) Indiana (East)
15 (GMT-04:00) Atlantic Time (Canada)
16 (GMT-04:00) Caracas, La Paz
17 (GMT-04:00) Santiago
18 (GMT-03:00) NewFoundland
19 (GMT-03:00) Brasilia
20 (GMT-03:00) Buenos Aires, Georgetown
21 (GMT-03:00) Greenland
22 (GMT-02:00) Mid-Atlantic
23 (GMT-01:00) Azores
24 (GMT-01:00) Cape Verde Is.
25 (GMT) Casablanca, Monrovia
26 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
27 (GMT+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
28 (GMT+01:00) Belgrade, Bratislava, Budapest, Ljubljana, Prague
29 (GMT+01:00) Brussels, Copenhagen, Madrid, Paris
30 (GMT+01:00) Sarajevo, Skopje, Sofija, Vilnius, Warsaw, Zagreb
31 (GMT+01:00) West Central Africa
32 (GMT+02:00) Athens, Istanbul, Minsk
33 (GMT+02:00) Bucharest
34 (GMT+02:00) Cairo
35 (GMT+02:00) Harare, Pretoria
36 (GMT+02:00) Helsinki, Riga, Tallinn
37 (GMT+02:00) Jerusalem
38 (GMT+03:00) Baghdad
39 (GMT+03:00) Kuwait, Riyadh

40 (GMT+03:00) Moscow, St. Petersburg, Volgograd
41 (GMT+03:00) Nairobi
42 (GMT+03:30) Tehran
43 (GMT+04:00) Abu Dhabi, Muscat
44 (GMT+04:00) Baku, Tbilisi, Yerevan
45 (GMT+04:30) Kabul
46 (GMT+05:00) Ekaterinburg
47 (GMT+05:00) Islamabad, Karachi, Tashkent
48 (GMT+05:30) Calcutta, Chennai, Mumbai, New Delhi
49 (GMT+05:45) Kathmandu
50 (GMT+06:00) Almaty, Novosibirsk
51 (GMT+06:00) Astana, Dhaka
52 (GMT+06:00) Sri Jayawardenepura
53 (GMT+06:30) Rangoon
54 (GMT+07:00) Bangkok, Hanoi, Jakarta
55 (GMT+07:00) Krasnoyarsk
56 (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi
57 (GMT+08:00) Irkutsk, Ulaan Bataar
58 (GMT+08:00) Kuala Lumpur, Singapore
59 (GMT+08:00) Perth
60 (GMT+08:00) Taipei
61 (GMT+09:00) Osaka, Sapporo, Tokyo
62 (GMT+09:00) Seoul
63 (GMT+09:00) Yakutsk
64 (GMT+09:30) Adelaide
65 (GMT+09:30) Darwin
66 (GMT+10:00) Brisbane
67 (GMT+10:00) Canberra, Melbourne, Sydney
68 (GMT+10:00) Guam, Port Moresby
69 (GMT+10:00) Hobart
70 (GMT+10:00) Vladivostok
71 (GMT+11:00) Magadan, Solomon Is., New Caledonia
72 (GMT+12:00) Aukland, Wellington
73 (GMT+12:00) Fiji, Kamchatka, Marshall Is.
74 (GMT+13:00) Nuku'alofa

Daylight Saving Time: click the check box to enable the Daylight Saving Function as the setting of start and end time or disable it.
Daylight Saving Start and **Daylight Saving End:** the time setting allows user to selects the week that monthly basis, and sets the End and Start time individually.



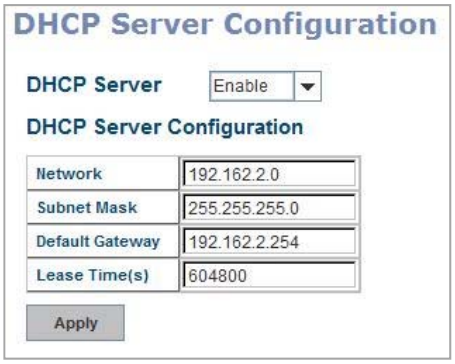
Once you finish your configuration, click on **Apply** to activate your configuration.

4.2.5 DHCP Server

You can select to **Enable** or **Disable** DHCP Server function. *PMI switch* will assign a new IP address to link partners.

DHCP Server configuration

After selecting to enable DHCP Server function, type in the Network IP address for the DHCP server IP pool, Subnet Mask, Default Gateway address and Lease Time for client.



Once you have finished the configuration, click **Apply** to activate the new configuration.

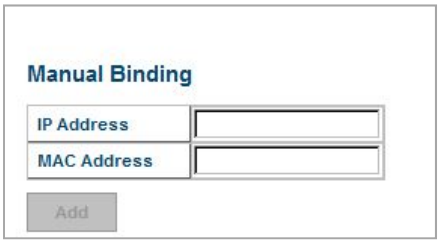
Excluded Address:

You can type a specific address into the **IP Address field** for the DHCP server reserved IP address.

The IP address that is listed in the **Excluded Address List Table** will not be assigned to the network device. Add or remove an IP address from the **Excluded Address List** by clicking **Add** or **Remove**.

Manual Binding: *PMI Switch* provides a MAC address and IP address binding and removing function. You can type in the specified IP and MAC address, and then click **Add** to add a new MAC&IP address binding rule for a specified link partner, like PLC or any device without

DHCP client function. To remove from the binding list, just select the rule to remove and click **Remove**.

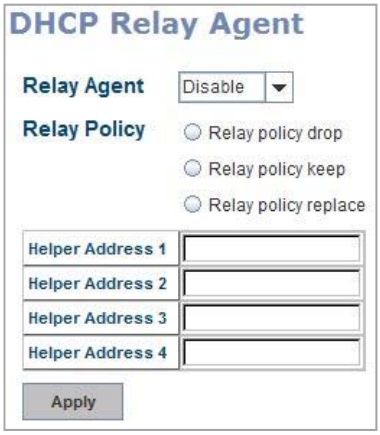


DHCP Leased Entries: *PMI Switch* provides an assigned IP address list for user check. It will show the MAC and IP

address that was assigned by *PMI Switch*. Click the **Reload** button to refresh the listing.

DHCP Relay Agent

You can select to **Enable** or **Disable** DHCP relay agent function, and then select the modification type of option 82 field.



Relay policy drop: Drops the option 82 field and do not add any option 82 field.

Relay policy keep: Keeps the original option 82 field and forwards to server.

Relay policy replace: Replaces the existing option 82 field and adds new option 82 field. (This is the default setting)

Helper Address: there are 4 fields for the DHCP server's IP address. You can filll the field with prefered IP address of DHCP Server, and then click "Apply" to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the policy and forwarded to DHCP server through the gateway port.

4.2.6 Backup and Restore

With Backup command, you can save current configuration file saved in the switch's flash to admin PC or TFTP server. This will allow you to go to **Restore** command later to restore the configuration file back to the switch. Before you restore the configuration file, you must place the backup configuration file in the PC or TFTP server. The switch will then download this file back to the flash.

There are 2 modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to backup the configuration. Users can also browse the target folder and select existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.

TFTP Server mode: In this mode, the switch acts as TFTP client. Before you do so, make sure that your TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

TFTP Server IP Address: You need to key in the IP address of your TFTP Server here.

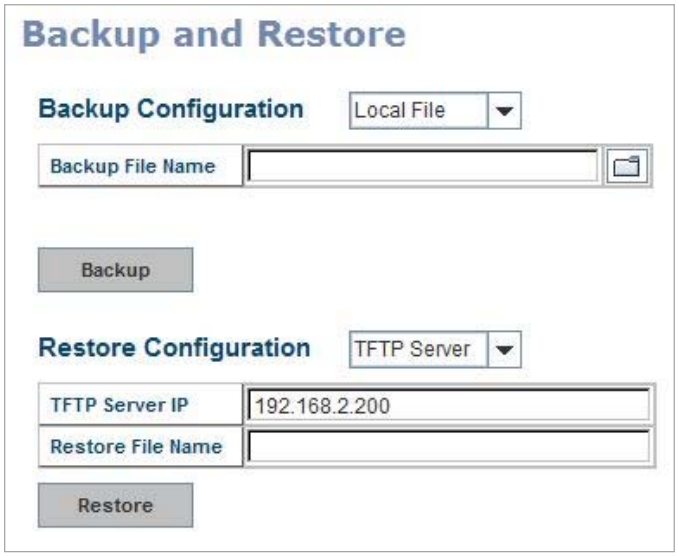
Backup/Restore File Name: Please type the correct file name of the configuration file.

Configuration File: The configuration file of the switch is a pure text file. You can open it by word/txt read file. You can also modify the file, add/remove the configuration settings, and then restore back to the switch.

Startup Configuration File: After you saved the running-config to flash, the new settings will be kept and work after power cycle. You can use *show startup-config* to view it in CLI. The Backup command can only backup such configuration file to your PC or TFTP server.

> ***Technical Tip:***
>
> ***Default Configuration File:*** *The switch provides the default configuration file in the system. You can use Reset button, Reload command to reset the system.*
>
> ***Running Configuration File:*** *The switch's CLI allows you to view the latest settings running by the system. The information shown here is the settings you set up but haven't saved to flash. The settings not yet saved to flash will not work after power recycle. You can* use *show running-config* to view it in CLI.

Once you finish selecting and configuring the settings, click on **Backup** or **Restore** to run



Click on the Folder icon to select the target file you want to backup/restore.

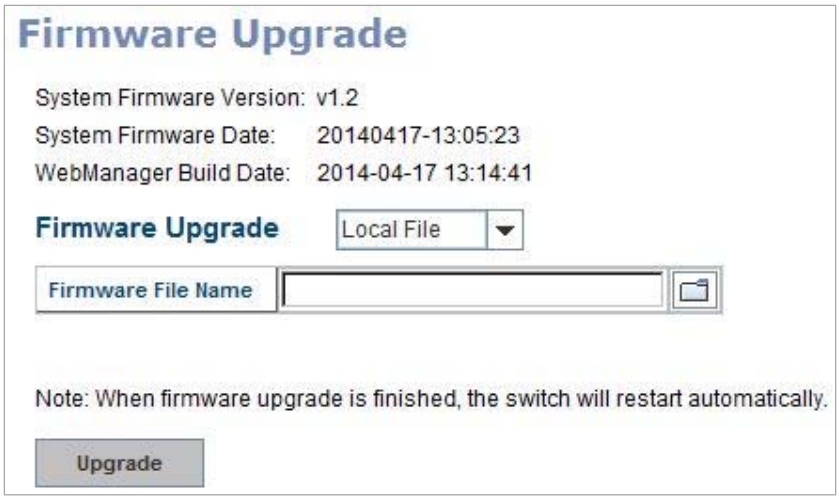
Note that the folders of the path to the target file do not allow you to input space key.

Type the IP address of TFTP Server IP. Then click on **Backup/Restore**.
Note: point to the wrong file will cause the entire configuration missed

4.2.7 Firmware Upgrade

In this section, you can update the latest firmware for your switch. Westermo provides the latest firmware in Westermo Web site. The new firmware may include new features, bug fixes or other software changes. We'll also provide the release notes for the update as well. For technical viewpoint, we suggest you use the latest firmware before installing the switch to the customer site.

Note that the system will be automatically rebooted after you finished upgrading new firmware. Please remind the attached network users before you perform this function.



There are 2 modes for users to backup/restore the configuration file, Local File mode and TFTP Server mode.

Local File mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to backup the configuration. Users also can browse the target folder and select the existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.

TFTP Server mode: In this mode, the switch acts as the TFTP client. Before you do so, make sure that your TFTP server is ready. And then please type the IP address of TFTP Server IP address. This mode can be used in both CLI and Web UI.

TFTP Server IP Address: You need to key in the IP address of your TFTP Server here.

Firmware File Name: The file name of the new firmware.
The UI also shows you the current firmware version and built date of current firmware. Please check the version number after the switch is rebooted.

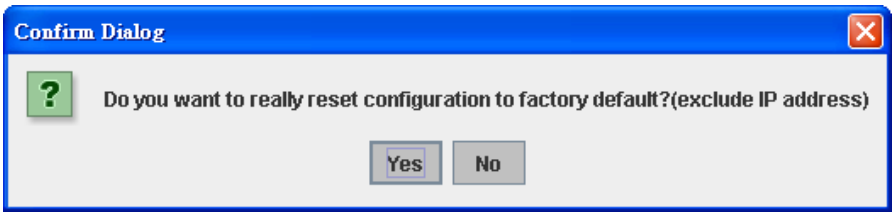
Click on the Folder icon to select the target firmware file you want to upgrade.

Type the IP address of TFTP Server and Firmware File Name. Then click on **Upgrade** to start the process.

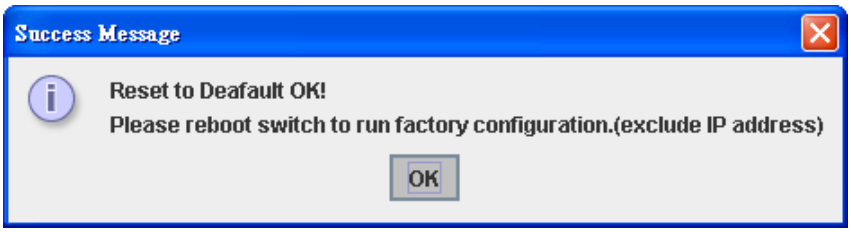
After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash. The CLI show …… until the process is finished.

4.2.8 Factory Default

In this section, you can reset all the configurations of the switch to default setting. Click on **Reset** the system will then reset all configurations to default setting. The system will show you popup message window after finishing this command. Default setting will work after rebooting the switch.



Click on **OK** to close the screen. Then please go to **Reboot** page to reboot the switch.



Click on **OK.** The system will then auto reboot the device.

Note: If you already configured the IP of your device to other IP address, when you use this command by CLI and Web UI, our software will not reset the IP address to default IP. The system will remain the IP address so that you can still connect the switch via the network.

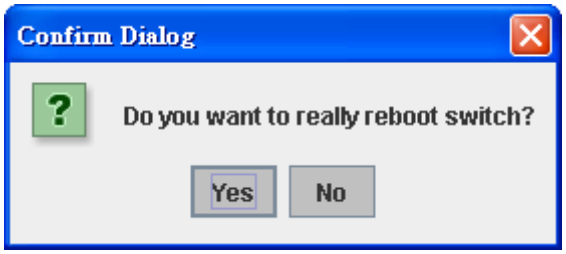
4.2.9 System Reboot

System Reboot allows you to reboot the device. Some of the feature changes require you to reboot the system. Click on **Reboot** to reboot your device.

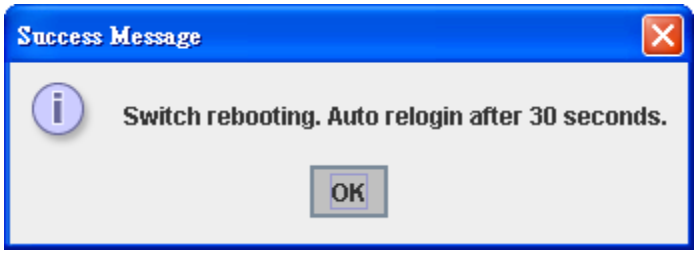
Note: *Remember to click on* ***Save*** *button to save your settings. Otherwise, the*

settings you made will be gone when the switch is powered off.

Click on **Yes**. Then the switch will be rebooted immediately.



Pop-up message screen appears when rebooting the switch..



4.2.10 CLI Commands for Basic Setting

Feature	Command Line
Switch Setting	
System Name	Switch(config)# hostname WORD Network name of this system Switch(config)# hostname “Switch” SWITCH(config)#
System Location	SWITCH(config)# snmp-server location Sweden
System Contact	SWITCH(config)# snmp-server contact support@westermo.se
Display	SWITCH# show snmp-server name SWITCH SWITCH# show snmp-server location Sweden SWITCH# show snmp-server contact

	support@westermo.se SWITCH> show version 0.31-20061218 Switch# show hardware mac MAC Address : 00:07:7c:e6:00:00
Admin Password	
User Name and Password	SWITCH(config)# administrator NAME Administrator account name SWITCH(config)# administrator orwell PASSWORD Administrator account_name account_password SWITCH(config)# administrator orwell orwell Change administrator account orwell and password orwell success.
Display	SWITCH# show administrator Administrator account information name: super password: super
IP Configuration	
IP Address/Mask (192.168.2.8, 255.255.255.0	SWITCH(config)# int vlan 1 SWITCH(config-if)# ip address dhcp SWITCH(config-if)# ip address 192.168.2.8/24 SWITCH(config-if)# ip dhcp client SWITCH(config-if)# ip dhcp client renew Switch(config-if)# ipv6 address ; IPv6 configuration X:X::X:X/M IPv6 address (e.g. 3ffe:506::1/48) Switch(config-if)# ipv6 address 3ffe:506::1/48
Gateway	SWITCH(config)# ip route 0.0.0.0/0 192.168.2.254/24
Remove Gateway	SWITCH(config)# no ip route 0.0.0.0/0 192.168.2.254/24
Display	SWITCH# show running-config …… ! interface vlan1 ip address 192.168.2.8/24 no shutdown ! ip route 0.0.0.0/0 192.168.2.254/24 !
Time Setting	
NTP Server	SWITCH(config)# ntp peer enable disable primary secondary SWITCH(config)# ntp peer primary IPADDR SWITCH(config)# ntp peer primary 192.168.2.200
Time Zone	SWITCH(config)# clock timezone 26 Sun Jan 1 04:13:24 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

	Note: By typing clock timezone ?, you can see the timezone list. Then choose the number of the timezone you want to select.
Daylight Saving	Switch(config)# **clock summer-time 4 0 2 12:00 4 0 3 12:00** **Clock summer-time** <*start week of month* > <*start weekday*> <*start month*> <*start Hour:Min*> <*end week of month*> <*end weekday*> <*end month*> <*end Hour:Min*> Start week of month: 1~5 Start weekday: 0 (Sunday) ~6 (Saturday) Month: 1 (Jan) ~12 (Dec)
IEEE 1588	Switch(config)# ptpd run <cr> preferred-clock Preferred Clock slave Run as slave
Display	SWITCH# sh ntp associations Network time protocol Status : Disabled Primary peer : N/A Secondary peer : N/A SWITCH# show clock Sun Jan 1 04:14:19 2006 (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London SWITCH# show clock timezone clock timezone (26) (GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
DHCP Server	
DHCP Server configuration	Enable DHCP Server on PMI Switch Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Configure DHCP network address pool Switch(config-dhcp)#network 50.50.50.0/4 -(network/mask) Switch(config-dhcp)#default-router 50.50.50.1
Lease time configure	Switch(config-dhcp)#lease 300 (300 sec)
DHCP Relay Agent	Enable DHCP Relay Agent Switch# Switch# configure terminal Switch(config)# router dhcp Switch(config-dhcp)# service dhcp Switch(config-dhcp)# ip dhcp relay information option Enable DHCP Relay policy Switch(config-dhcp)# ip dhcp relay information policy replace drop Relay Policy keep Drop/Keep/Replace option82 field replace
Show DHCP server information	Switch# show ip dhcp server statistics Switch# show ip dhcp server statistics DHCP Server ON

	Address Pool 1 network:192.168.2.0/24 default-router:192.168.2.254 lease time:300 Excluded Address List IP Address ---------- (list excluded address) Manual Binding List IP Address MAC Address ---------- ---------- (list IP & MAC binding entry) Leased Address List IP Address MAC Address Leased Time Remains ---------- ---------- ---------- (list leased Time remain information for each entry)
Backup and Restore	
Backup Startup Configuration file	Switch# copy startup-config tftp: 192.168.2.33/default.conf Writing Configuration [OK] ***Note 1:*** *To backup the latest startup configuration file, you should save current settings to flash first. You can refer to 4.12 to see how to save settings to the flash.* *Note 2: 192.168.2.33 is the TFTP server's IP and default.conf is name of the configuration file. Your environment may use different IP addresses or different file name. Please type target TFTP server IP or file name in this command.*
Restore Configuration	Switch# copy tftp: 192.168.2.33/default.conf startup-config
Show Startup Configuration	Switch# show startup-config
Show Running Configuration	Switch# show running-config
Firmware Upgrade	
Firmware Upgrade	Switch# archive download-sw /overwrite tftp 192.168.2.33 pmi-110.bin → **binary code file name** Firmware upgrading, don't turn off the switch! Tftping file pmi-110.bin → **binary code file name** Firmware upgrading .... Firmware upgrade success!! Rebooting.....
Factory Default	
Factory Default	Switch# reload default-config file Reload OK! Switch# reboot
System Reboot	
Reboot	Switch# reboot

4.3 Port Configuration

Port Configuration group enables you to enable/disable port state, or configure port auto-negotiation, speed, and duplex, flow control, rate limit control and port aggregation settings. It also allows you to view port status and aggregation information.

Following commands are included in this group:

4.3.1 Port Control

4.3.2 Port Status

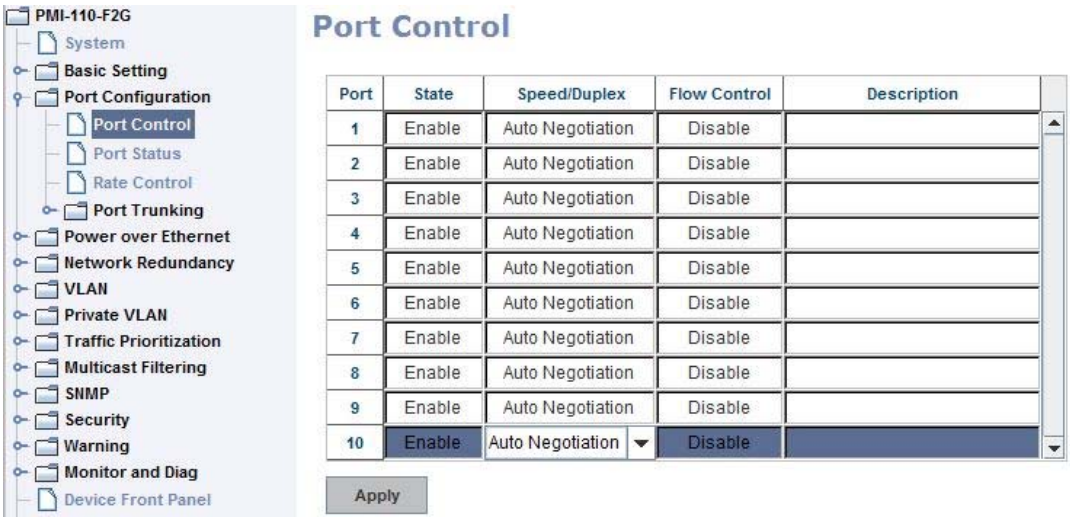
4.3.3 Rate Control

4.3.4 Port Trunking

4.3.5 Command Lines for Port Configuration

4.3.1 Port Control

Port Control commands allow you to enable/disable port state, or configure the port auto-negotiation, speed, duplex and flow control.



Select the port you want to configure and make changes to the port.

In **State** column, you can enable or disable the state of this port. Once you disable, the port stop to link to the other end and stop to forward any traffic. The default setting is Enable which means all the ports are workable when you receive the device.

In **Speed/Duplex** column, you can configure port speed and duplex mode of this port. Below are the selections you can choose:

Fast Ethernet Port 1~8 (fa1~fa8): AutoNegotiation, 10M Full Duplex (10 Full), 10M Half Duplex (10 Half), 100M Full Duplex (100 Full) and 100M Half Duplex (100 Half).

Gigabit Ethernet Port 9~10: (gi9~gi10): AutoNegotiation, 10M Full Duplex (10 Full), 10M Half Duplex (10 Half), 100M Full Duplex (100 Full), 100M Half Duplex

(100 Half), 1000M Full Duplex (1000 Full), 1000M Half Duplex (1000 Half).

The default mode is Auto Negotiation mode.

In **Flow Control** column, “Symmetric” means that you need to activate the flow control function of the remote network device in order to let the flow control of that corresponding port on the switch to work. “Disable” means that you don’t need to activate the flow control function of the remote network device, as the flow control of that corresponding port on the switch will work anyway.

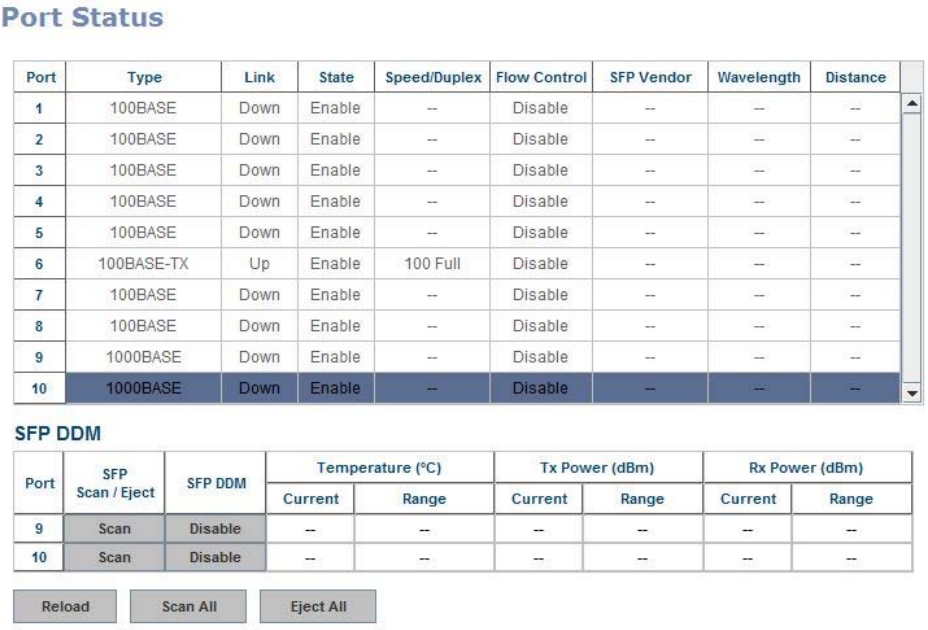
Description: the description of interface. It supports maximum characters length is 130.

Once you finish configuring the settings, click on **Apply** to save the configuration.

Technical Tips: *If both ends are not at the same speed, they can’t link with each other. If both ends are not in the same duplex mode, they will be connected by half mode.*

4.3.2 Port Status

Port Status shows you current port status.


Port Status
Port Type Link State Speed/Duplex Flow Control SFP Vendor Wavelength Distance
1 100BASE Down Enable -- Disable -- -- --
2 100BASE Down Enable -- Disable -- -- --
3 100BASE Down Enable -- Disable -- -- --
4 100BASE Down Enable -- Disable -- -- --
5 100BASE Down Enable -- Disable -- -- --
6 100BASE-TX Up Enable 100 Full Disable -- -- --
7 100BASE Down Enable -- Disable -- -- --
8 100BASE Down Enable -- Disable -- -- --
9 1000BASE Down Enable -- Disable -- -- --
10 1000BASE Down Enable -- Disable -- -- --
SFP DDM
Port SFP Scan / Eject SFP DDM Temperature (°C) Tx Power (dBm) Rx Power (dBm)
Current Range Current Range Current Range
9 Scan Disable -- -- -- -- -- --
10 Scan Disable -- -- -- -- -- --
Reload Scan All Eject All

The description of the columns is as below:

SFP Vendor: Vendor name of the SFP transceiver you plugged.

Wavelength: The wave length of the SFP transceiver you plugged.

Distance: The distance of the SFP transceiver you plugged.

Reload: reload the all port information.

Scan all: scan the SFP transceiver and display.

Eject: Eject the SFP transceiver that you have selected. You can eject one port or eject all by click the icon “Eject All”.

Temperature: The temperature spcific and current detected of DDM SFP transceiver.

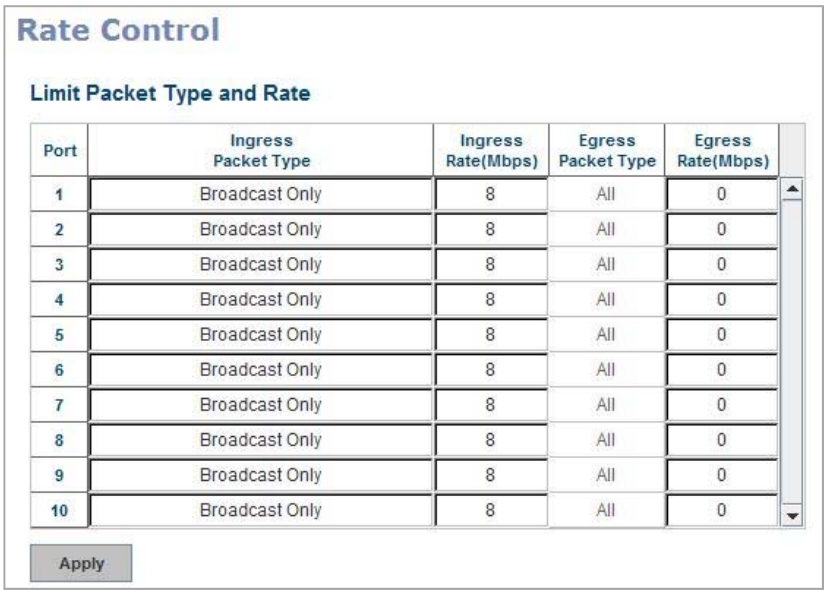
Tx Power (dBm): The specification and current transmit power of DDM SFP transceiver.

Rx Power (dBm): The specification and current received power of DDM SFP transceiver.

Note: 1. Most of the SFP transceivers provide vendor information which allows your switch to read it. The UI can display vendor name, wave length and distance of all Westermo SFP transceiver family. If you see Unknown info, it may mean that the vendor doesn't provide their information or that the information of their transceiver can't be read.

2. if the plugged DDM SFP transceiver is not certified by Westermo, the DDM function will not be supported. But the communication still works.

4.3.3 Rate Control


Rate Control
Limit Packet Type and Rate
Port
Ingress Packet Type
Ingress Rate(Mbps)
Egress Packet Type
Egress Rate(Mbps)
1 Broadcast Only 8 All 0
2 Broadcast Only 8 All 0
3 Broadcast Only 8 All 0
4 Broadcast Only 8 All 0
5 Broadcast Only 8 All 0
6 Broadcast Only 8 All 0
7 Broadcast Only 8 All 0
8 Broadcast Only 8 All 0
9 Broadcast Only 8 All 0
10 Broadcast Only 8 All 0
Apply

Rate limiting is a form of flow control used to enforce a strict bandwidth limit at a port. You can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types as described below.

Packet type: You can select the packet type that you want to filter. The packet types of the Ingress Rule listed here include **Broadcast Only** / **Broadcast and multicast** / **Broadcast, Multicast and Unknown Unicast** or **All**. The packet types of the Egress Rule (outgoing) only support **all** packet types.

Rate: This column allows you to manually assign the limit rate of the port. Valid values are from 1Mbps-100Mbps for fast Ethernet ports and gigabit Ethernet ports. The step of the rate is 1 Mbps. Default value of Ingress Rule is "8" Mbps; default value of Egress Rule is 0 Mbps. 0 stands for disabling the rate control for the port.

Click on **Apply** to apply the configuration.

4.3.4 Port Trunking

Port Trunking configuration allows you to group multiple Ethernet ports in parallel to increase link bandwidth. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. Port Trunking feature is usually used when you need higher bandwidth for backbone network. This is an inexpensive way for you to transfer more data.

There are some different descriptions for the port trunking. Different manufacturers may use different descriptions for their products, like Link Aggregation Group (LAG), Link Aggregation Control Protocol, Ethernet Trunk, Ether Channel…etc. Most of the implementations now conform to IEEE standard, 802.3ad.

The aggregated ports can interconnect to the other switch which also supports Port Trunking. Westermo Supports 2 types of port trunking. One is Static Trunk, the other is 802.3ad. When the other end uses 802.3ad LACP, you **should** assign 802.3ad LACP to the trunk. When the other end uses non-802.3ad, you can then use Static Trunk.

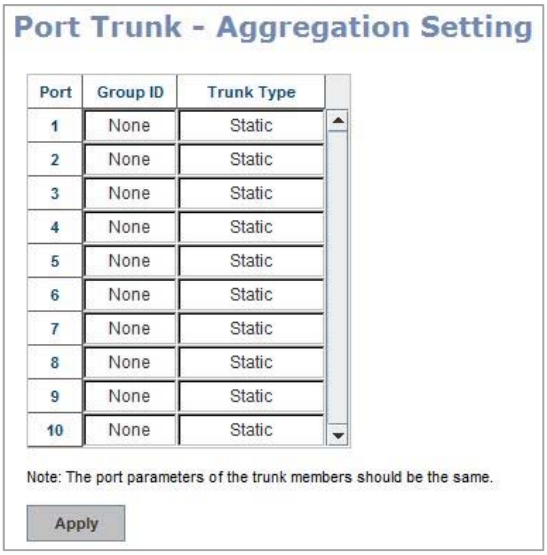
There are 2 configuration pages, Aggregation Setting and Aggregation Status.

Aggregation Setting

Trunk Size: The switch can support up to 8 trunk groups with 2 trunk members. Since the member ports should use same speed/duplex, max trunk members for 100Mbps would be 8, and 2 for gigabit.

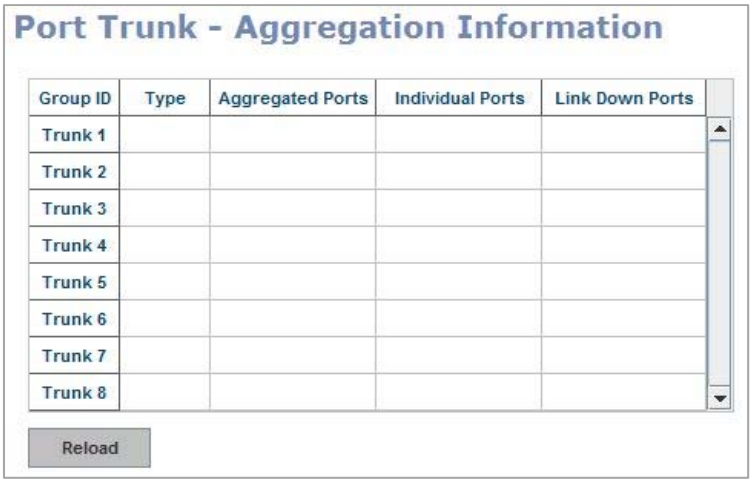
Group ID: Group ID is the ID for the port trunking group. Ports with same group ID are in the same group.

Type: Static and **802.3ad LACP.** Each Trunk Group can only support Static or 802.3ad LACP. Choose the type you need here.



Aggregation Status

This page shows the status of port aggregation. Once the aggregation ports are negotiated well, you will see following status.



Group ID: Display Trunk 1 to Trunk 5 set up in Aggregation Setting.
Type: Static or LACP set up in Aggregation Setting.
Aggregated: When LACP links well, you can see the member ports in aggregated column.
Individual: When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports will be displayed in the Individual column.
Link Down: When LACP is enabled, member ports of LACP group which are not linked up will be displayed in the Link Down column.

4.3.5 Command Lines for Port Configuration

Feature	Command Line
Port Control	
Port Control – State	Switch(config-if)# shutdown -> Disable port state Port1 Link Change to DOWN interface fastethernet1 is shutdown now. Switch(config-if)# no shutdown -> Enable port state Port1 Link Change to DOWN Port1 Link Change to UP interface fastethernet1 is up now. Switch(config-if)# Port1 Link Change to UP
Port Control – Auto Negotiation	Switch(config)# interface fa1 Switch(config-if)# auto-negotiation Auto-negotiation of port 1 is enabled!
Port Control – Force Speed/Duplex	Switch(config-if)# speed 100 Port1 Link Change to DOWN set the speed mode ok! Switch(config-if)# Port1 Link Change to UP Switch(config-if)# duplex full Port1 Link Change to DOWN set the duplex mode ok! Switch(config-if)# Port1 Link Change to UP

Port Control – Flow Control	Switch(config-if)# flowcontrol on Flowcontrol on for port 1 set ok! Switch(config-if)# flowcontrol off Flowcontrol off for port 1 set ok!
Port Status	
Port Status	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Connected Duplex : Full Speed : 100 Flow Control :off Default Port VLAN ID: 1 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Disable Loopback Mode : None STP Status: forwarding Default CoS Value for untagged packets is 0. Mdix mode is Disable. Medium mode is Copper. *Note: Administrative Status -> Port state of the port. Operating status -> Current status of the port. Duplex -> Duplex mode of the port. Speed -> Speed mode of the port. Flow control -> Flow Control status of the port.*
Rate Control	
Rate Control – Ingress or Egress	Switch(config-if)# rate-limit egress Outgoing packets ingress Incoming packets ***Note: To enable rate control, you should select the Ingress or Egress rule first; then assign the packet type and bandwidth.***
Rate Control – Filter Packet Type	Switch(config-if)# rate-limit ingress mode all Limit all frames broadcast Limit Broadcast frames flooded-unicast Limit Broadcast, Multicast and flooded unicast frames multicast Limit Broadcast and Multicast frames Switch(config-if)# rate-limit ingress mode broadcast Set the ingress limit mode broadcast ok.
Rate Control - Bandwidth	Switch(config-if)# rate-limit ingress bandwidth <0-100> Limit in magabits per second (0 is no limit) Switch(config-if)# rate-limit ingress bandwidth 8 Set the ingress rate limit 8Mbps for Port 1.
Port Trunking	
LACP	Switch(config)# lacp group 1 gi8-10 Group 1 based on LACP(802.3ad) is enabled! *Note: The interface list is fa1,fa3-5,gi8-10* Note: different speed port can't be aggregated together.

Static Trunk	Switch(config)# trunk group 2 fa6-7 Trunk group 2 enable ok!
Display - LACP	PMI Switch# show lacp internal LACP group 1 internal information: LACP Port Admin Oper Port Port Priority Key Key State ----- ----------- -------- -------- ------- 8 1 8 8 0x45 9 1 9 9 0x45 10 1 10 10 0x45 LACP group 2 is inactive LACP group 3 is inactive LACP group 4 is inactive
Display - Trunk	Switch# show trunk group 1 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports --------+---------+----------------------------------- 1 LACP 8(D) 9(D) 10(D) Switch# show trunk group 2 FLAGS: I -> Individual P -> In channel D -> Port Down Trunk Group GroupID Protocol Ports --------+---------+----------------------------------- 2 Static 6(D) 7(P) Switch#

4.4 Power over Ethernet

Power over Ethernet is the key features of *PMI* PoE Switch. It is fully compliance with IEEE 802.3af and IEEE 802.3at that include 1-event with IEEE 802.1AB LLDP classification and 2-event classification mechanisms for PoE MDI. The *PMI-110-F2G adapts* 8-Port PoE injectors in port 1 to port 8, each port with the ability to deliver 30W to compatible IEEE 802.3at standard and provides 120w power budget for hall system. Therefore, select and install the PoE PD system is The following commands are included in this section:

4.4.1 PoE Control
4.4.2 PoE Scheduling
4.4.3 PoE Status
4.4.4 Command Line for PoE control

4.4.1 PoE Control

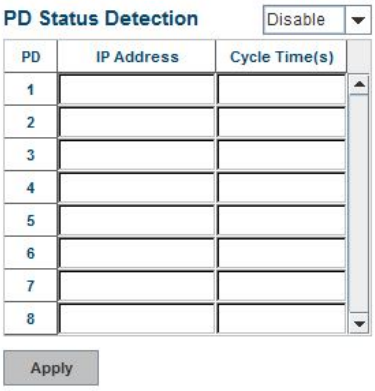
The PoE contrl includes 3 parts- **PoE System**, **Port configuration** and **PD status detection**. The following will iintroduce the function.

PoE System Dialogue

PoE System: enable or disable system's PoE function.
Budget (W): the power supply maximum output budget. Both power budget of DC 1 and DC2 will be aggregated.
Voltage (V): the voltage of applied to the power input. Here, we suggest uses same specification of power supply. If the power supply with different output voltage, it may casue system draw more current from one power model which with higher voltage.
Warning Water Level (%): the warning level is for system warning to alerts user when PoE system drawing power that meet the warning level user defined.

Port Configuration Dialogue

PoE Mode: Enable/Diable port's PoE function.
Powering Mode: 802.3af, 802.3at(LLDP), 802.3at(2-event) and forced mode. Forced mode will ignore the classification behaviors and apply power onto the RJ-45, uses the forced mode must be carefully.
Power Budget(W): it allows user assigne the budget control in this field.
Power priority: it supports 3 levels, Critical, High and low. If the system PoE consumption is over the system budgte control, the PoE system will turn off low priorty port PoE function, until the consumption is becomes smaller than the system budget.



PD Status Detection Diaglogue

The PMI PoE Switch supports an useful function that help user to mainten the PD's status and help use to savng the maintenance time and money.

IP address: the PD's ipaddress that installed on the port.
Cycle time: user measured the PD system boots duration time. The unit is second. Most of PD system – IP camera will take at least 40~50 seconds. Here, we suggest user sets the cycle time to 90 seconds prevents any wrong suppose.

Once user defined this function, the PoE Switch will request PD system and turn-off PoE power if PD system does not echo the request. After the duration time (cycle time), the PoE switch will start request PD again. This function also named **link partner line detection (LPLD)**.

Note: During the PoE operating, the surface will accumulate heat and caused surface temperature becomes higher than ambient temperature. Do remember don't touch device surface during PoE operating.

DO NOT TOUCH DEVICE SURFACE DURING PoE PROGRESS HIGH POWER FEEDING

Note: To enable the IEEE 802.3at High Power PoE function, the power input voltage should be DC 52~57V to obtain better performance. Applies DC 48V to PoE Switch and perform 30W high power output may cause the PoE disable

automatically, due the output current protect mechanism activated (0.686A current limite). To avoid this issue, we suggest adjust the power supply output to 52V DC or higher. In usually, the Switching power supply adopted adjust resistor for voltage fine tune.

4.4.2 PoE Scheduling

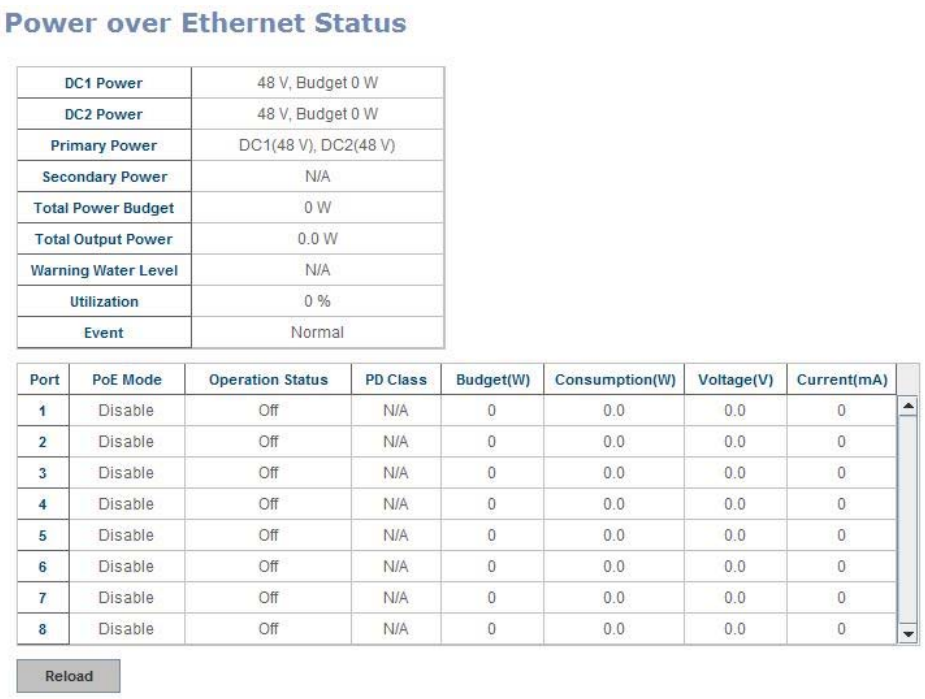
The PoE Scheduling control is a powerful function to help you save power and money. You need to configure **PoE Scheduling** and select a target port manually to enable this function.

The Power over Ethernet schedule supports hourly and weekly base PoE schedule configuration.

Selecte the target port and marking the time frame, then click **Apply** to activate the PoE scheduling function. The PoE port will working as the predefined behavior and follows the system clock. As this result, be sure the system clock have configured as your local time for the reference of scheduling control.

4.4.3 PoE Status

The PoE Status page shows the system PoE status and the operating status of each PoE Port. The information includes PoE mode, Operation status, and PD class, Power Consumption, Voltage and Current. For system information, it includes the setting of system power budget, PoE system output power, setting of warning level, utilization of system power and event.


Power over Ethernet Status
DC1 Power 48 V, Budget 0 W
DC2 Power 48 V, Budget 0 W
Primary Power DC1(48 V), DC2(48 V)
Secondary Power N/A
Total Power Budget 0 W
Total Output Power 0.0 W
Warning Water Level N/A
Utilization 0 %
Event Normal
Port PoE Mode Operation Status PD Class Budget(W) Consumption(W) Voltage(V) Current(mA)
1 Disable Off N/A 0 0.0 0.0 0
2 Disable Off N/A 0 0.0 0.0 0
3 Disable Off N/A 0 0.0 0.0 0
4 Disable Off N/A 0 0.0 0.0 0
5 Disable Off N/A 0 0.0 0.0 0
6 Disable Off N/A 0 0.0 0.0 0
7 Disable Off N/A 0 0.0 0.0 0
8 Disable Off N/A 0 0.0 0.0 0
Reload

4.4.4 Command Line for PoE control

Syntax	**show poe system**
Parameters	--
Command Mode	Enable mode
Description	Display the status of the PoE system.
Examples	Switch> enable Switch# show poe system PoE System PoE Admin : Enable PoE Hardward : Normal PoE Input Voltage : 47.700 V Output power : 0.00 Watts Power Budget : Budget : 120 Watts Warning water level : N/A Utilization : 0 % Event : Normal
Syntax	**show poe interface** IFNAME
Parameters	IFNAME : interface name
Command Mode	Enable mode
Description	Display the PoE status of interface.
Examples	Switch> enable Switch# show poe interface fa1 Interface fastethernet1 (POE Port 1) Control Mode : User (Disable) Powering Mode : 802.3af Operation Status : Off

	Detection Status : Valid Classification : N/A Priority : Highest Output Power : 0.0 Watts, Voltage : 0.0 V, Current : 0 mA Power Budget : Budget : 32.0 Watts, effective 0 Watts Warning water level : N/A Utilization : 0 % Event : Normal
Syntax	**show poe pd_detect**
Parameters	--
Command Mode	Enable mode
Description	Display the status of pd status detection.
Examples	Switch# show poe pd-detect PD Status Detection Status : Enabled Host 1 : Target IP : 192.168.2.100 Cycle Time : 10 Host 2 : Target IP : 192.168.2.200 Cycle Time : 20 Host 3 : Target IP : 192.168.2.15 Cycle Time : 30 Host 4 : Target IP : 192.168.2.20 Cycle Time : 40
Syntax	**show poe schedule IFNAME**
Parameters	IFNAME : interface name
Command Mode	Enable mode
Description	Display the status of schedule of interface.
Examples	Switch# show poe schedule fa1 Interface fastethernet1 POE Schedule Status : Disable Weekly Schedule : Sunday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Monday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Tuesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Wednesday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Thursday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Friday : 0,1,2,3,4,5,6,7,8,19,20,21,22,23 Saturday : 0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20
Syntax	**poe powering-mode 802.3af/forced**
Parameters	802.3af: deliver power if and only if the attached PD comply with IEEE 802.3af forced: deliver power no maater what PD attached
Command Mode	Interface mode
Description	Set the Powring mode of PoE

Examples	EX 1: *Set 802.3af powring mode* Switch(config)# poe powering-mode 802.3af EX 2: *Set forced powering mode* Switch(config)# poe powering-mode forced
Syntax	**poe powering-mode 802.3at 2-event/lldp**
Parameters	2-event: deliver power if and only if the attached PD comply with IEEE 802.3at physical layer classification lldp: deliver power if and only if the attached PD comply with IEEE 802.3at data link layer classification
Command Mode	Interface mode
Description	Set the Powring mode of PoE
Examples	EX 1: *Set 802.3at 2-event powring mode* Switch(config)# poe powering-mode 802.3at 2-event EX 2: *Set 802.3at lldpforced powering mode* Switch(config)# poe powering-mode 802.3at lldp
Syntax	**poe control-mode user/schedule**
Parameters	user: user mode schedule: schedule mode
Command Mode	Interface mode
Description	Set the control mode of port
Examples	Set PoE port 2 to user mode. EX 1: Switch(config)# interface fa2 Switch(config-if)# poe control-mode user Set PoE port 2 to schedule mode. EX 2: Switch(config-if)# poe control-mode schedule
Syntax	**poe user enable/disable**
Parameters	enable: enable port in user mode disable: disable port in user mode
Command Mode	Interface mode
Description	Enable/Disable the PoE of the port in user mode. If in schedule mode, it will come into affect when the control mode changes to user mode.
Examples	To enable the PoE function in user mode Switch(config-if)# poe user enable To disable the PoE function in user mode Switch(config-if)# poe user disable
Syntax	**poe type TYPE**
Parameters	TYPE : port type string with max 20 characters
Command Mode	Interface mode
Description	Set the port type string.
Examples	Set the type string to “IPCam-1. Switch(config-if)# poe type IPCam-1
Syntax	**poe budget [POWER]**
Parameters	POWER : 0.4 – 30
Command Mode	Interface mode
Description	Set the port budget.

	The max budget is different between 802.3af, 802,3at and forced powering mode. The max budget of 802.3af powering mode is 15.4. The max budget of 802.3at powering mode is 30 The max budget of force powering mode is 30.
Examples	Set the max value of power consumption to 12 W with manual mode. Switch(config-if)# poe budget 12
Syntax	**poe budget warning <0-100>**
Parameters	<0-100> 0 is disable, valid range is 1 to 100 percentage
Command Mode	Interface mode
Description	Set the warning water level of port budget.
Examples	Set the warning water level to 60% Switch(config-if)# poe budget warning 60
Syntax	**poe priority critical/high/low**
Parameters	Critical : Hightest priority level High : High priority level Low : Low priority level
Command Mode	Interface mode
Description	Set the powering priority. The port with higher priority will have the privilege to delivery power under limited power situation.
Examples	Set the priority to critical Switch(config-if)# poe priority critical
Syntax	**poe schedule weekday hour**
Parameters	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, …, 6=Saturday) Hour : Valid range 0-23, Valid format a,b,c-d
Command Mode	Interface mode
Description	Add a day schedule to an interface.
Examples	Add a schedule which enables PoE function at hour 1, 3, 5 and 10 to 23 on Sunday. Switch(config-if)# poe schedule 0 1,3,5,10-23
Syntax	**no poe schedule** weekday
Parameters	Weekday : Valid range 0-6 (0=Sunday, 1=Monday, …, 6=Saturday)
Command Mode	Interface mode
Description	Remove a day schedule
Examples	Remove the Sunday schedule. Switch(config-if)# no poe schedule 0
Syntax	**poe budget DC1/DC2 [POWER] ; system command for PMI-110-F2G is 120Watts under 70C operating temperature.**
Parameters	POWER : 0~200
Command Mode	Configuration mode
Description	Set the power budget of DC1
Examples	Set the power budget of DC1 to 200W Switch(config)# poe budget DC1 200w
Syntax	**poe budget warning <0-100>**
Parameters	<0-100> 0 is disable, valid range is 1 to 100 percentage
Command Mode	Configuration mode

Description	Set the warning water level of total power budget.
Examples	Set the warning water level to 60% Switch(config-if)# poe budget warning 60
Syntax	**poe pd_detect enable/disable**
Parameters	enable: enable PD Status Detection function disable: disable PD Status Detection function
Command Mode	Configuration mode
Description	Enable/Disable the PD Status Detection function
Examples	To enable the function of pd status detect function Switch(config)# poe pd_detect enable To disable the function of pd status detect function Switch(configf)# poe pd_detect disable
Syntax	**poe pd_detect ip_address cycle_time**
Parameters	IP address : A.B.C.D Cycle time : Valid range 10-3600 second and must be multiple of 10
Command Mode	Configuration mode
Description	Apply a rule of PD Status Detection.
Examples	Apply a rule which ping 192.160.1.2 per 20 seconds. And if 192.160.1.2 is timeout, pd status detection will re-enable the PoE. Switch(config)# poe pd_detect 192.160.1.2 20

4.5 Network Redundancy

It is critical for industrial applications that network remains non-stop. PMI Switch supports standard RSTP, Multiple Super Ring, Rapid Dual Homing and backward compatible with Legacy Super Ring Client modes.

Multiple Super Ring (MSR) technology, 0 ms for restore and about 5 milliseconds for failover for copper.

Advanced Rapid Dual Homing (RDH) technology also facilitates PMI Switch to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP cloud together, which is also known as Auto Ring Coupling.

To become backwards compatible with the Legacy Super Ring technology implemented in *PMI* switches, PMI Switch also supports Super Ring Client mode. The Super Ring ports can pass through Super Ring control packets extremely well and works with Super Ring.

Besides ring technology, *all PMI Managed Switch* support 802.1D-2004 version Rapid Spanning Tree Protocol (RSTP). New version of RSTP standard includes 802.1D-1998 STP, 802.1w RSTP, IEEE 802.1s MSTP (Multiple Spanning Tree). The MSTP function is available from 1.1 version firmwear.

Following commands are included in this group:

4.5.1 STP configuration

4.5.2 STP Port configuration

4.5.3 STP information

4.5.4 MSTP configuration

4.5.5 MSTP Port Configuration

4.5.6 MSTP information

4.5.7 Multiple Super Ring

4.5.8 Multiple Super Ring Info

4.5.9 Command Lines for Network Redundancy

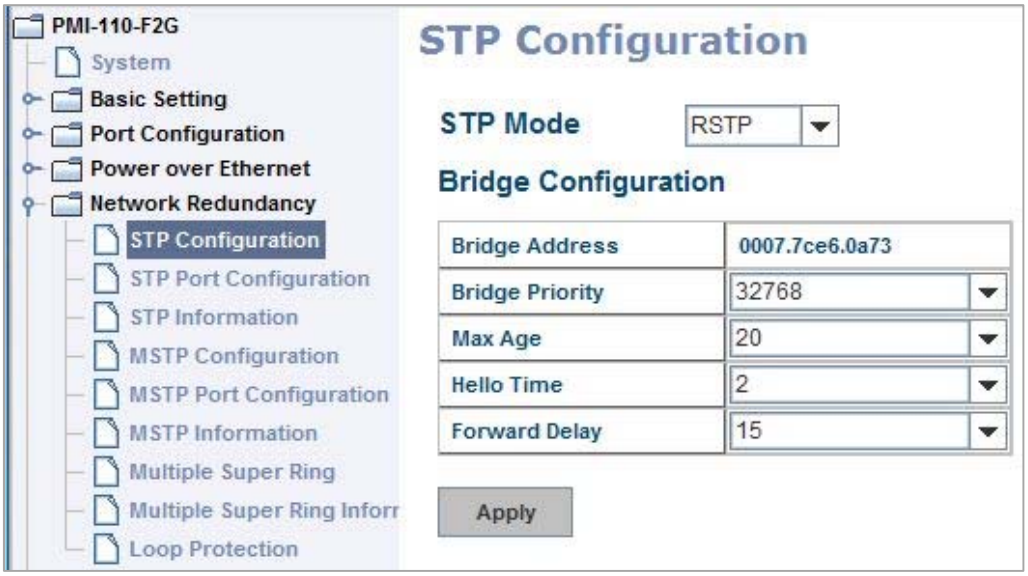
4.5.1 STP Configuration

This page allows select the STP mode and configuring the global STP/RSTP Bridge Configuraiton.

The STP mode includes the **STP**, **RSTP**, **MSTP** and **Disable**. Please select the STP mode for your system first. The default mode is RSTP enabled.

Afte select the STP or RSTP mode; continue to configure the gloable Bridge parameters for STP and RSTP.

After select the MSTP mode, please go to MSTP Configuration page.



RSTP is the abbreviation of Rapid Spanning Tree Protocol. If a switch has more than one path to a destination, it will lead to message loops that can generate broadcast storms and quickly bog down a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree uses a spanning tree algorithm (STA) to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path (primary), and block the other path(s). It will also keep track of the blocked path(s) in case the primary path fails. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. It is specified in IEEE 802.1D-1998. Later, Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change. This is specified in IEEE 802.1w. In 2004, 802.1w is included into 802.1D-2004 version. This switch supports both RSTP and STP (all switches that support RSTP are also backward compatible with switches that support only STP).

Bridge Configuration

Bridge Address: This shows the switch's MAC address.

Priority (0-61440): RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will then become the root bridge.

Note: The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority. Ex: 4096 is higher than 32768.

Note: The Web GUI allows user select the priority number directly. This is the convinent of the GUI design. When you configure the value through the CLI or SNMP, you may need to type the value directly. Please follow the n x 4096 ruls for the Bridge Priority.

Max Age (6-40): Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

If PMI is not the root bridge, and if it has not received a hello message from the root bridge in an amount of time equal to Max Age, then PMI will reconfigure itself as a root bridge. Once two or more devices on the network are recognized as a root bridge, the devices will renegotiate to set up a new spanning tree topology.

Hello Time (1-10): Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status.

The root bridge of the spanning tree topology periodically sends out a "hello" message to other devices on the network to check if the topology is "healthy". The "hello time" is the amount of time the root has waited during sending hello messages.

Forward Delay Time (4-30): Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

This is the amount of time PMI will wait before checking to see if it should be changed to a different state.

Once you have completed your configuration, click on **Apply** to apply your settings.

Note: You must observe the following rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

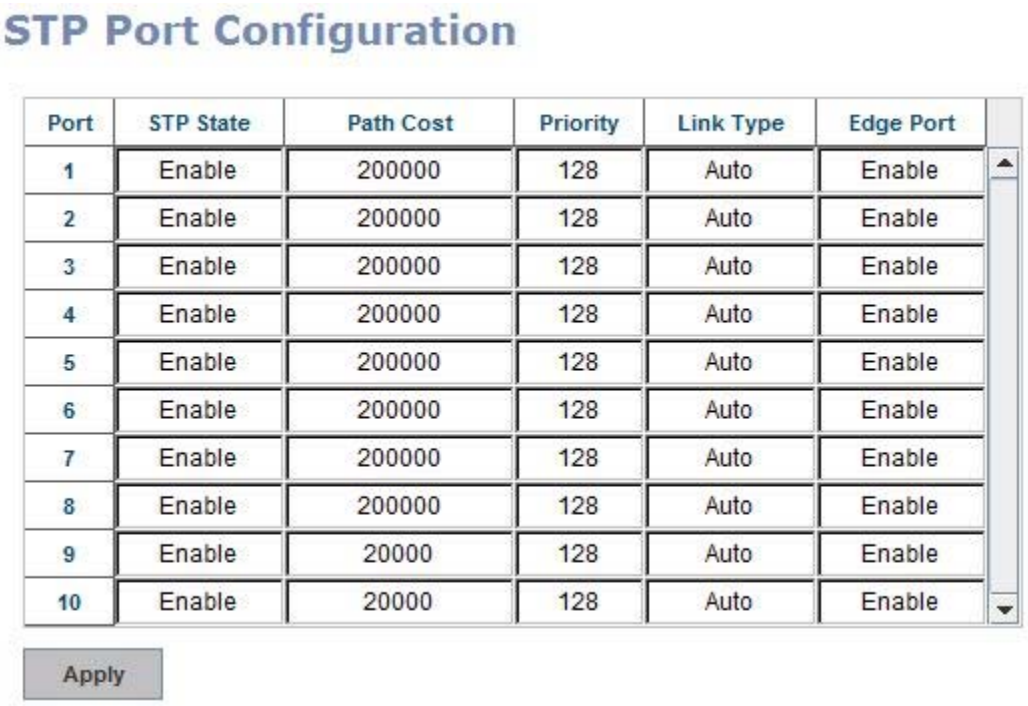
2 × (Forward Delay Time – 1 sec) ≥ Max Age Time ≥ 2 × (Hello Time value + 1 sec)

4.5.2 STP Port Configuration

This page allows you to configure the port parameter after enabled STP or RSTP.

Port Configuration

Select the port you want to configure and you will be able to view current setting and status of the port.


STP Port Configuration
Port
STP State
Path Cost
Priority
Link Type
Edge Port
1 Enable 200000 128 Auto Enable
2 Enable 200000 128 Auto Enable
3 Enable 200000 128 Auto Enable
4 Enable 200000 128 Auto Enable
5 Enable 200000 128 Auto Enable
6 Enable 200000 128 Auto Enable
7 Enable 200000 128 Auto Enable
8 Enable 200000 128 Auto Enable
9 Enable 20000 128 Auto Enable
10 Enable 20000 128 Auto Enable
Apply

Path Cost: Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

Priority: Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Link Type: There are 3 types for you select. **Auto, P2P** and **Share.**

Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. "**Auto**" means to auto select P2P or Share mode. "**P2P"** means P2P is enabled; the 2 ends work at Full-duplex mode. While "**Share"** is enabled, it means P2P is disabled, the 2 ends may connect through a share media and work in Half duplex mode.

Edge: A port directly connected to the end stations cannot create a bridging loop

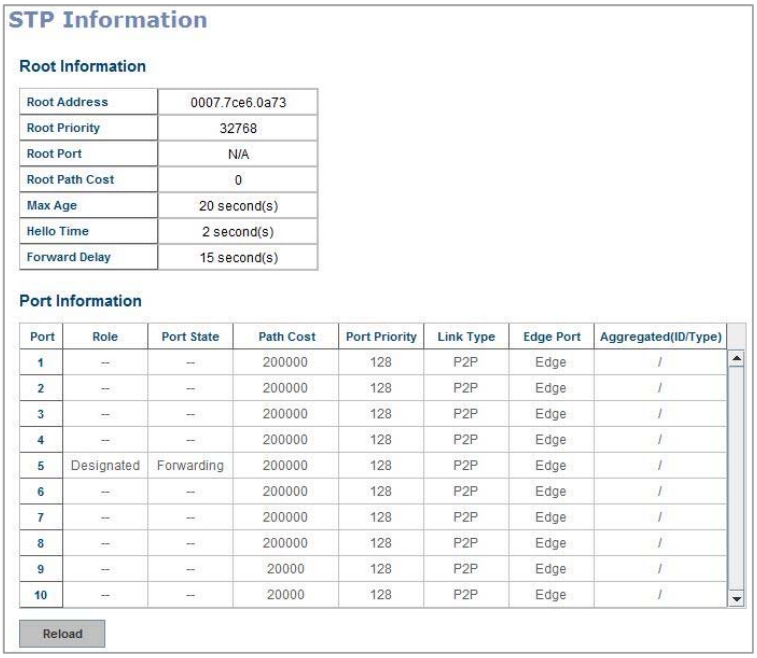
in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.

Once you finish your configuration, click on **Apply** to save your settings.

4.5.3 RSTP Info

This page allows you to see the information of the root switch and port status.

Root Information: You can see root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root


STP Information
Root Information
Root Address 0007.7ce6.0a73
Root Priority 32768
Root Port N/A
Root Path Cost 0
Max Age 20 second(s)
Hello Time 2 second(s)
Forward Delay 15 second(s)
Port Information
Port Role Port State Path Cost Port Priority Link Type Edge Port Aggregated(ID/Type)
1 -- -- 200000 128 P2P Edge /
2 -- -- 200000 128 P2P Edge /
3 -- -- 200000 128 P2P Edge /
4 -- -- 200000 128 P2P Edge /
5 Designated Forwarding 200000 128 P2P Edge /
6 -- -- 200000 128 P2P Edge /
7 -- -- 200000 128 P2P Edge /
8 -- -- 200000 128 P2P Edge /
9 -- -- 20000 128 P2P Edge /
10 -- -- 20000 128 P2P Edge /
Reload

switch.

Port Information: You can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode and Aggregated (ID/Type).

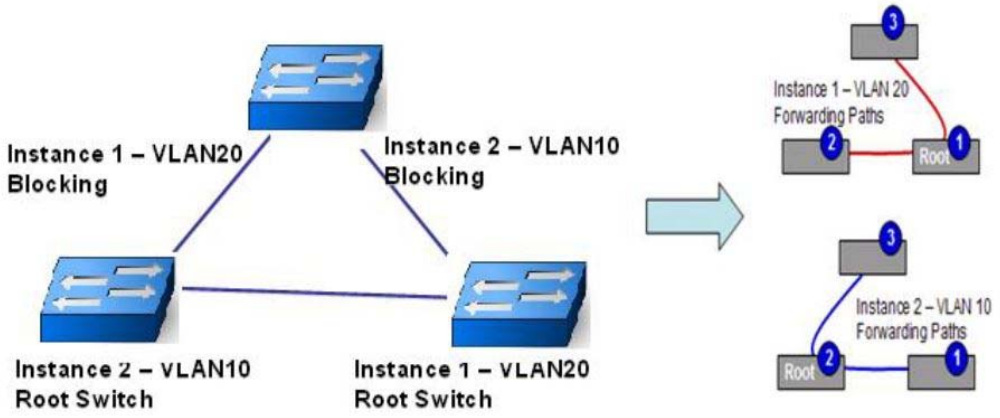
4.5.4 MSTP (Multiple Spanning Tree Protocol) Configuration

MSTP is the abbreviation of Multiple Spanning Tree Protocol. This protocol is a direct extension of RSTP. It can provide an independent spanning tree for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group (as sometimes occurs with IEEE 802.1D STP).

While using MSTP, there are some new concepts of network architecture. A switch may belong to different group, acts as root or designate switch, generate BPDU for the network to maintain the forwarding table of the spanning tree. With MSTP, it can also provide multiple forwarding paths and enable load balancing. Understand the architecture allows you to maintain the correct spanning tree and operate effectively.

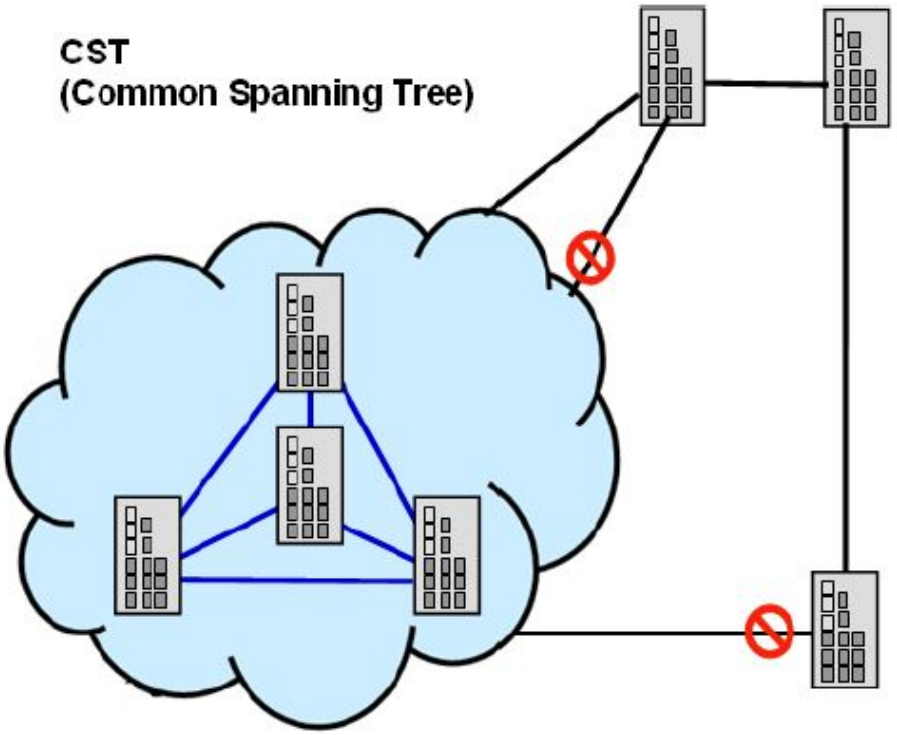
One VLAN can be mapped to a Multiple Spanning Tree Instance (MSTI). The maximum Instance of PMI Managed Switch support is 16, range from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

The figure shows there are 2 VLANs/MSTP Instances and each instance has its Root and forwarding paths.



A Common Spanning Tree (CST) interconnects all adjuacent MST regions and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network. MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

The figure shows the CST large network. In this network, a Region may have different instances and its own forwarding path and table; however, it acts as a single Brige of CST.



To configure the MSTP setting, the STP Mode of the STP Configuration page should be changed to MSTP mode first.

After enabled MSTP mode, then you can go to the MSTP Configuraiton pages.

MSTP Region Configuration

This page allows configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration. The network can be divided virtually to different Regions. The switches within the Region should have the same Region and Revision leve.

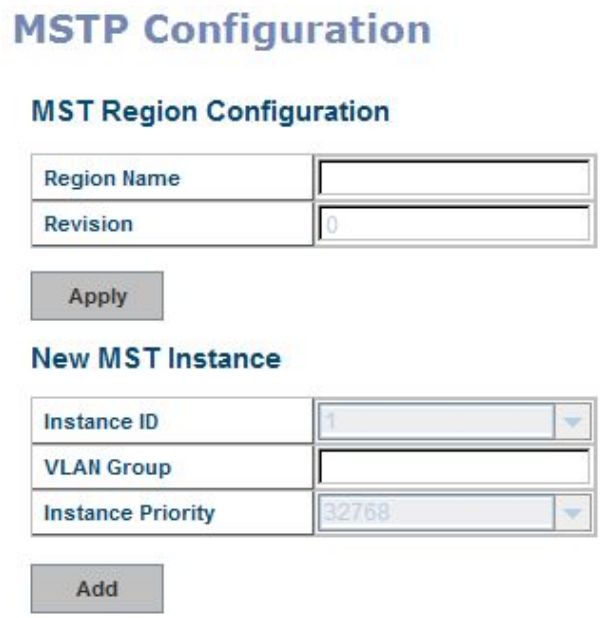
Region Name: The name for the Region. Maximum length: 32 characters.

Revision: The revision for the Region. Range: 0-65535; Default: 0)

Once you finish your configuration, click on **Apply** to apply your settings.

New MST Instance

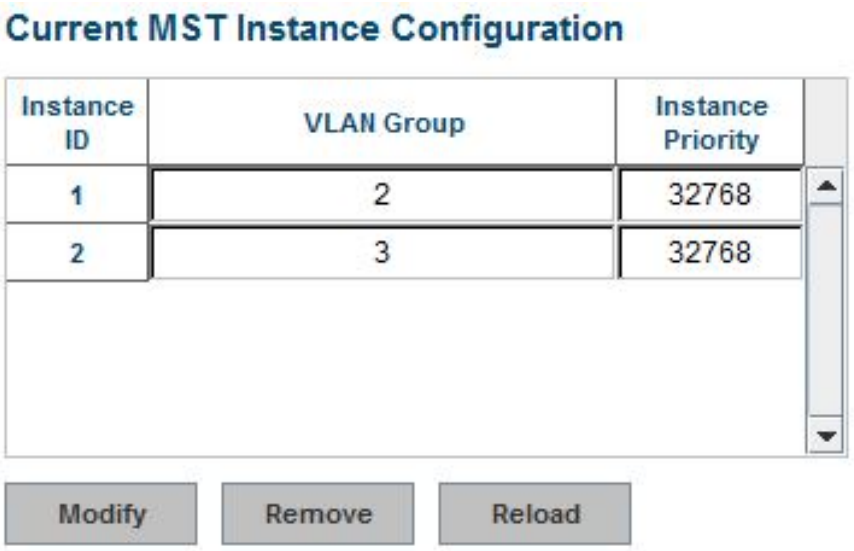
This page allows mapping the VLAN to Instance and assign priority to the instance. Before mapping VLAN to Instance, you should create VLAN and assign the member ports first. Please refer to the VLAN setting page.



Instance ID: Select the Instance ID, the available number is 1-15.
VLAN Group: Type the VLAN ID you want mapping to the instance.
Instance Priority: Assign the priority to the instance.
After finish your configuration, click on **Add** to apply your settings.

Current MST Instance Configuration

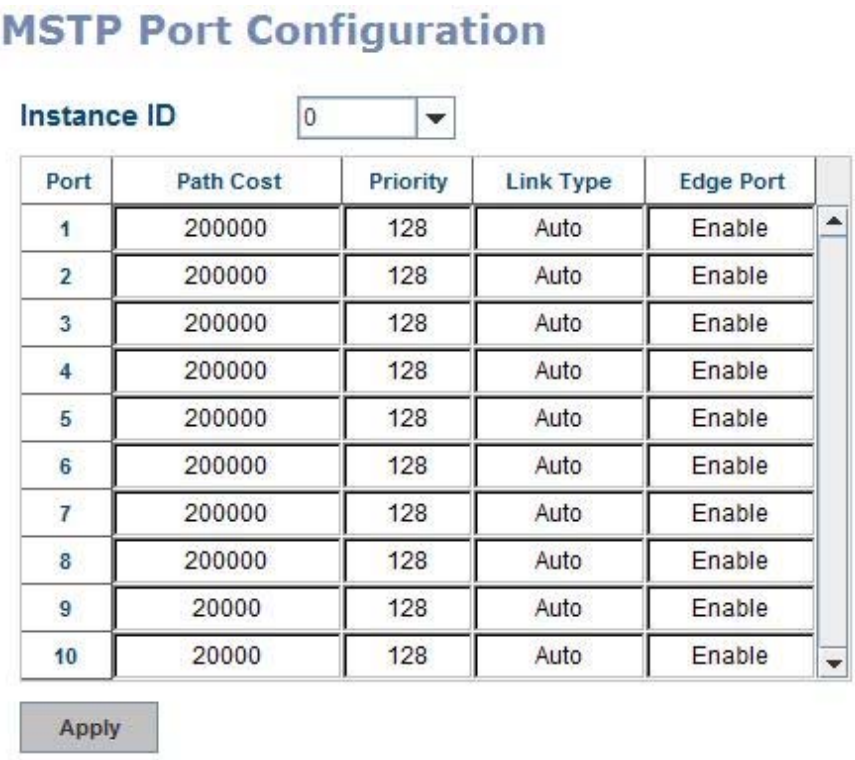
This page allows you to see the current MST Instance Configuration you added. Click on "**Apply**" to apply the setting. You can "**Remove"** the instance or "**Reload**" the configuration display in this page.



4.5.5 MSTP Port Configuration

This page allows configure the Port settings. Choose the Instance ID you want to configure. The MSTP enabled and linked up ports within the instance will be listed in this table.

Note that the ports not belonged to the Instance, or the ports not MSTP activated will not display. The meaning of the Path Cost, Priority, Link Type and Edge Port is the same as the definition of RSTP.



Path Cost: Enter a number between 1 and 200,000,000. This value represents the "cost" of the path to the other bridge from the transmitting bridge at the specified port.

Priority: Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.

Link Type: There are 3 types for you select. **Auto, P2P** and **Share.**

Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. "**Auto**" means to auto select P2P or Share mode. "**P2P"** means P2P is enabled; the 2 ends work in full duplex mode. While "**Share"** is enabled, it means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.

Edge: A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the **Enable** state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.

Once you finish your configuration, click on **Apply** to save your settings.

4.5.6 MSTP Information

This page allows you to see the current MSTP information.

Choose the **Instance ID** first. If the instance is not added, the information remains blank.

The **Root Information** shows the setting of the Root switch.

The **Port Information** shows the port setting and status of the ports within the instance.

Click "**Reload**" to reload the MSTP information display.

4.5.7 Multiple Super Ring (MSR)

The most common industrial network redundancy is to form a ring or loop. Typically, the managed switches are connected in series and the last switch is connected back to the first one. In such connection, you can implement Multiple Super Ring technology to get fatest recovery performance.

Multiple Super Ring (MSR) technology have a fast restore and failover time, 0 ms for restore and about milliseconds level for failover for 100Base-TX copper port. The other interface may take longer time due to the media characteristics.

Advanced **Rapid Dual Homing (RDH)** technology also facilitates *PMI Managed Switch* to connect with a core managed switch easily and conveniently. With RDH technology, you can also couple several Rapid Super Rings or RSTP cloud together, which is also known as Auto Ring Coupling.

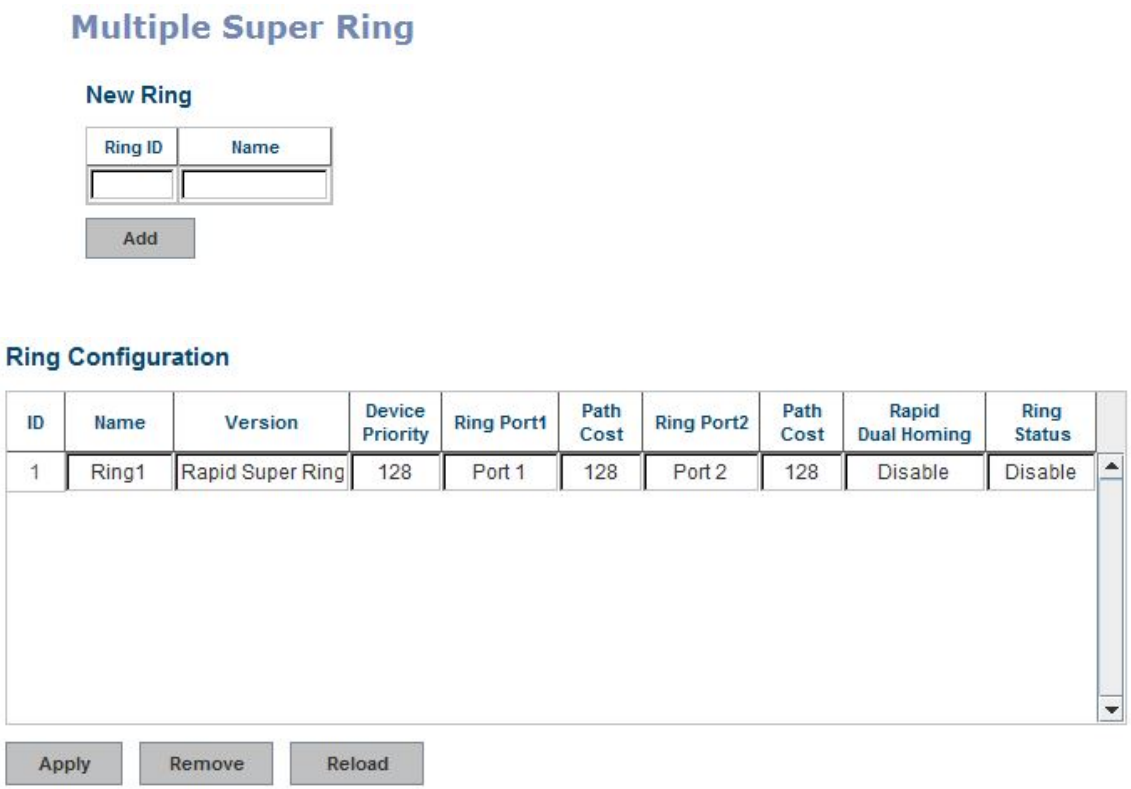
TrunkRing technology allows integrate MSR with LACP/Port Trunking. The LACP/Trunk aggregated ports is a virtual interface and it can work as the Ring port of the MSR.

MultiRing is an outstanding technology. Multiple rings can be aggregated within one switch by using different Ring ID. The maximum Ring number one switch can support is half of total port volume. For example, the PMI-110-F2G is a 10 port Ethernet Switch design, which means maximum 5 Rings (4 100Mbps + 1 Gigabit Rings) can be aggregated in one. The feature saves much effort when

constructing complex network architecture.

To become backwards compatible with the Legacy Super Ring technology implemented in *PMI Managed – PMI-110-F2G* switch also supports Super Ring Client mode. The Super Ring ports can pass through Super Ring control packets extremely well and works with Super Ring.

New Ring: To create a Rapdis Super Ring. Just fill in the Ring ID which has range from 0 to 31. If the name field is left blank, the name of this ring will be automatically naming with Ring ID.



Ring Configuration

ID: Once a Ring is created, This appears and can not be changed.

Name: This field will show the name of the Ring. If it is not filled in when creating, it will be automatically named by the rule “RingID”.

Version: The version of Ring can be changed here. There are three modes to choose: Rapid Super Ring as default; Super ring and Any Ring for compatible with other version of rings.

Device Priority: The switch with highest priority (highest value) will be automatically selected as Ring Master. Then one of the ring ports in this switch will become forwarding port and the other one will become blocking port. If all of the switches have the same priority, the switch with the biggest MAC address will be selected as Ring Master.

Ring Port1: In Rapid Super Ring environment, you should have 2 Ring Ports. No matter this switch is Ring Master or not, when configuring RSR, 2 ports should be

selected to be Ring Ports. For Ring Master, one of the ring ports will become the forwarding port and the other one will become the blocking port.

Path Cost: Change the Path Cost of Ring Port1. If this switch is the Ring Master of a Ring, then it determines the blocking port. The Port with higher Path Cost in the two ring ports will become the blocking port, If the Path Cost is the same, the port with larger port number will become the blocking port.

Ring Port2: Assign another port for ring connection

Path Cost: Change the Path Cost of Ring Port2

Rapid Dual Homing: Rapid Dual Homing is an important feature of the Ring redundancy technology. When you want to connect multiple RSR or form redundant topology with other vendors,RDH could allow you to have maximum 7 multiple links for redundancy without any problem.

In Dual Homing you have to configure additional port as Dual Homing port to two uplink switches. In Rapid Dual Homing, you don't need to configure specific port to connect to other protocol. The Rapid Dual Homing will smartly choose the fastest link for primary link and block all the other link to avoid loop. If the primary link failed, Rapid Dual Homing will automatically forward the secondary link for network redundant. Of course, if there are more connections, they will be standby links and recover one of then if both primary and secondary links are broken.

Ring status: To enable/disable the Ring. Please remember to enable the ring after you add it.

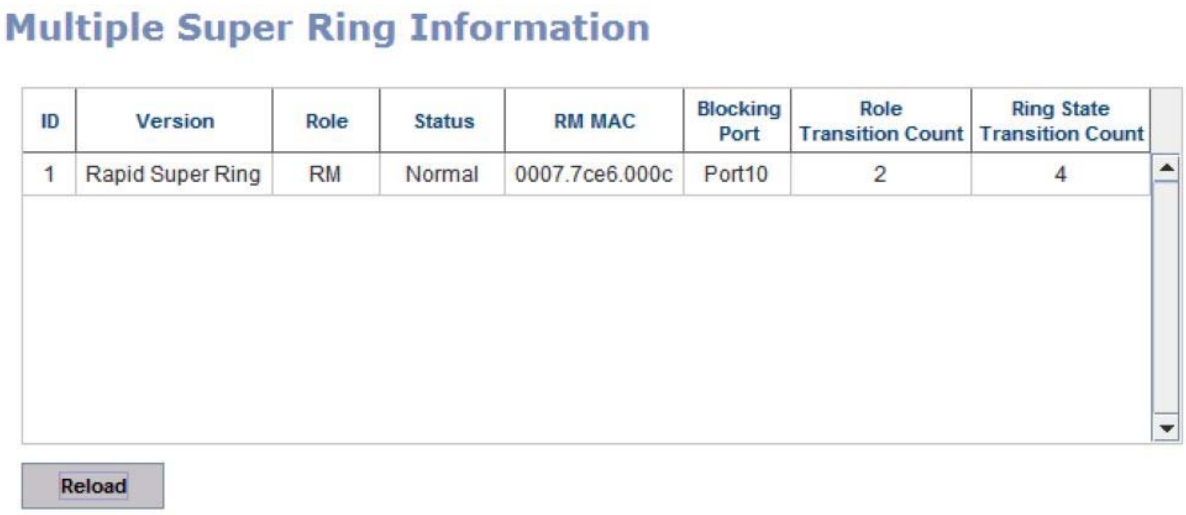
MultiRing: The MultiRing technology is one of the patterns of the MSR technology; it allows you to aggregate multiple rings within one switch. Create multiple ring ID and assign different ring port 1 and port 2 to each ring, thus the switch can have multiple rings in one PMI Switch.

When implementing MultiRing, remember that the different rings can NOT use the same ring ID. The other settings are the same as above description. Technically, the maximum ring volume the MultiRing supported is up to 16 rings. Due the limited number of ports, the number of ring network is the half of port number.

TrunkRing: The MultiRing technology is part of the MSR technology which combines the MSR with the port trunking technology. After multiple ports aggregated, this is so-call port trunking (Staticly or learnt by LACP protocol), the Trunk ID can be one of the port ID of the MSR technology. Configured the port trunking first then you can add the Trunk group as a Ring Port in managed switch.

4.5.8 Ring Info

This page shows the RSR information.



ID: Ring ID.

Version: which version of this ring, this field could be Rapid Super Ring, Super Ring, or Any Ring

Role: This Switch is RM or nonRM

Status: If this field is Normal which means the redundancy is approved. If any one of the link in this Ring is broken, then the status will be Abnormal.

RM MAC: The MAC address of Ring Master of this Ring. It helps to find the redundant path.

Blocking Port: This field shows which is blocked port of RM.

Role Transition Count: This means how many times this switch has changed its Role from nonRM to RM or from RM to nonRM.

Role state Transition Count: This number means how many times the Ring status has been transformed between Normal and Abnormal state.

4.5.9 Command Lines:

Feature	Command Line
Global (STP, RSTP, MSTP)	
Enable	Switch(config)# spanning-tree enable
Disable	Switch (config)# spanning-tree disable
Mode (Choose the Spanning Tree mode)	Switch(config)# spanning-tree mode rst the rapid spanning-tree protocol (802.1w) stp the spanning-tree prtotcol (802.1d) mst the multiple spanning-tree protocol (802.1s)
Bridge Priority	Switch(config)# spanning-tree priority <0-61440> valid range is 0 to 61440 in multiple of 4096 Switch(config)# spanning-tree priority 4096
Bridge Times	Switch(config)# spanning-tree bridge-times (forward Delay) (max-age) (Hello Time) Switch(config)# spanning-tree bridge-times 15 20 2 This command allows you configure all the timing in one time.
Forward Delay	Switch(config)# spanning-tree forward-time <4-30> Valid range is 4~30 seconds Switch(config)# spanning-tree forward-time 15
Max Age	Switch(config)# spanning-tree max-age <6-40> Valid range is 6~40 seconds Switch(config)# spanning-tree max-age 20
Hello Time	Switch(config)# spanning-tree hello-time <1-10> Valid range is 1~10 seconds Switch(config)# spanning-tree hello-time 2
MSTP	
Enter the MSTP Configuration Tree	Switch(config)# spanning-tree mst MSTMAP the mst instance number or range configuration enter mst configuration mode forward-time the forward dleay time hello-time the hello time max-age the message maximum age time max-hops the maximum hops sync sync port state of exist vlan entry Switch(config)# spanning-tree mst configuration Switch(config)# spanning-tree mst configuration Switch(config-mst)# abort exit current mode and discard all changes end exit current mode, change to enable mode and apply all changes exit exit current mode and apply all changes instance the mst instance list Print command list name the name of mst region no Negate a command or set its defaults quit exit current mode and apply all changes revision the revision of mst region show show mst configuration
Region Configuration	Region Name: Switch(config-mst)# name NAME the name string Switch(config-mst)# name Westermo

	Region Revision: Switch(config-mst)# revision <0-65535> the value of revision Switch(config-mst)# revision 65535
Mapping Instance to VLAN (Ex: Mapping VLAN 2 to Instance 1)	Switch(config-mst)# instance <1-15> target instance number Switch(config-mst)# instance 1 vlan VLANMAP target vlan number(ex.10) or range(ex.1-10) Switch(config-mst)# instance 1 vlan 2
Display Current MST Configuraion	Switch(config-mst)# show current Current MST configuration Name [Westermo] Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094 1 2 2 3 ---------- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
Remove Region Name	Switch(config-mst)# no name name configure revision revision configure instance the mst instance Switch(config-mst)# no name
Remove Instance example	Switch(config-mst)# no instance <1-15> target instance number Switch(config-mst)# no instance 2
Show Pending MST Configuration	Switch(config-mst)# show pending Pending MST configuration Name [] (->The name is removed by no name) Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,3-4094 1 2 (->Instance 2 is removed by no instance 2) ---------- Config HMAC-MD5 Digest: 0x3AB68794D602FDF43B21C0B37AC3BCA8 ----------
Apply the setting and go to the configuration mode	Switch(config-mst)# quit apply all mst configuration changes Switch(config)#
Apply the setting and go to the global mode	Switch(config-mst)# end apply all mst configuration changes Switch#
Abort the Setting and go to the configuration mode. Show Pending to see the new settings are not applied.	Switch(config-mst)# abort discard all mst configuration changes Switch(config)# spanning-tree mst configuration Switch(config-mst)# show pending Pending MST configuration Name [Westermo] (->The nameis not applied after Abort settings.) Revision 65535 Instance Vlans Mapped -------- ----------

	0 1,4-4094 1 2 2 3 (-> The instance is not applied after Abort settings.) --- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ---
RSTP	
System RSTP Setting	The mode should be rst, the timings can be configured in global settings listed in above.
Port Configuration Mode	
Port Configuraiton	Switch(config)# interface fa1 Switch(config-if)# spanning-tree bpdufilter a secure BPDU process on edge-port interfcae bpduguard a secure response to invalid configurations(received BPDU sent by self) cost change an interafce's spanning-tree port path cost edge-port interface attached to a LAN segment that is at the end of a bridged LAN or to an end node link-type the link type for the Rapid Spanning Tree mst the multiple spanning-tree port-priority the spanning tree port priority
Port Path Cost	Switch(config-if)# spanning-tree cost <1-200000000> 16-bit based value range from 1-65535, 32-bit based value range from 1-200,000,000 Switch(config-if)# spanning-tree cost 200000
Port Priority	Switch(config-if)# spanning-tree port-priority <0-240> Number from 0 to 240, in multiple of 16 Switch(config-if)# spanning-tree port-priority 128
Link Type - Auto	Switch(config-if)# spanning-tree link-type auto
Link Type - P2P	Switch(config-if)# spanning-tree link-type point-to-point
Link Type – Share	Switch(config-if)# spanning-tree link-type shared
Edge Port	Switch(config-if)# spanning-tree edge-port enable Switch(config-if)# spanning-tree edge-port disable
MSTP Port Configuration	Switch(config-if)# spanning-tree mst MSTMAP cost <1-200000000> the value of mst instance port cost Switch(config-if)# spanning-tree mst MSTMAP port-priority <0-240> the value of mst instance port priority in multiple of 16
Global Information	
Active Information	Switch# show spanning-tree active Spanning-Tree : Enabled Protocol : MSTP Root Address : 0012.77ee.eeee Priority : 32768 Root Path Cost : 0 Root Port : N/A Root Times : max-age 20, hello-time 2, forward-delay 15 Bridge Address : 0012.77ee.eeee Priority : 32768 Bridge Times : max-age 20, hello-time 2, forward-delay 15 BPDU transmission-limit : 3 Port Role State Cost Prio.Nbr Type Aggregated --- fa1 Designated Forwarding 200000 128.1 P2P(RSTP) N/A fa2 Designated Forwarding 200000 128.2 P2P(RSTP) N/A
RSTP Summary	Switch# show spanning-tree summary Switch is in rapid-stp mode. BPDU skewing detection disabled for the bridge. Backbonefast disabled for bridge.

	Summary of connected spanning tree ports : #Port-State Summary Blocking Listening Learning Forwarding Disabled -------- --------- -------- ---------- -------- 0 0 0 2 8 #Port Link-Type Summary AutoDetected PointToPoint SharedLink EdgePort ------------ ------------ ---------- -------- 9 0 1 9
Port Info	Switch# show spanning-tree port detail fa7 (Interface_ID) Rapid Spanning-Tree feature Enabled Port 128.6 as Disabled Role is in Disabled State Port Path Cost 200000, Port Identifier 128.6 RSTP Port Admin Link-Type is Auto, Oper Link-Type is Point-to-Point RSTP Port Admin Edge-Port is Enabled, Oper Edge-Port is Edge Designated root has priority 32768, address 0012.7700.0112 Designated bridge has priority 32768, address 0012.7760.1aec Designated Port ID is 128.6, Root Path Cost is 600000 Timers : message-age 0 sec, forward-delay 0 sec Link Aggregation Group: N/A, Type: N/A, Aggregated with: N/A BPDU: sent 43759 , received 4854 TCN : sent 0 , received 0 Forwarding-State Transmit count 12 Message-Age Expired count
MSTP Information	
MSTP Configuraiton	Switch# show spanning-tree mst configuration Current MST configuration (MSTP is Running) Name [Westermo] Revision 65535 Instance Vlans Mapped -------- ---------- 0 1,4-4094 1 2 2 3 ---------- Config HMAC-MD5 Digest: 0xB41829F9030A054FB74EF7A8587FF58D ----------
Display all MST Information	Switch# show spanning-tree mst ###### MST00 vlans mapped: 1,4-4094 Bridge address 0012.77ee.eeee priority 32768 (sysid 0) Root this switch for CST and IST Configured max-age 2, hello-time 15, forward-delay 20, max-hops 20 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ---------- fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP) ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ----------

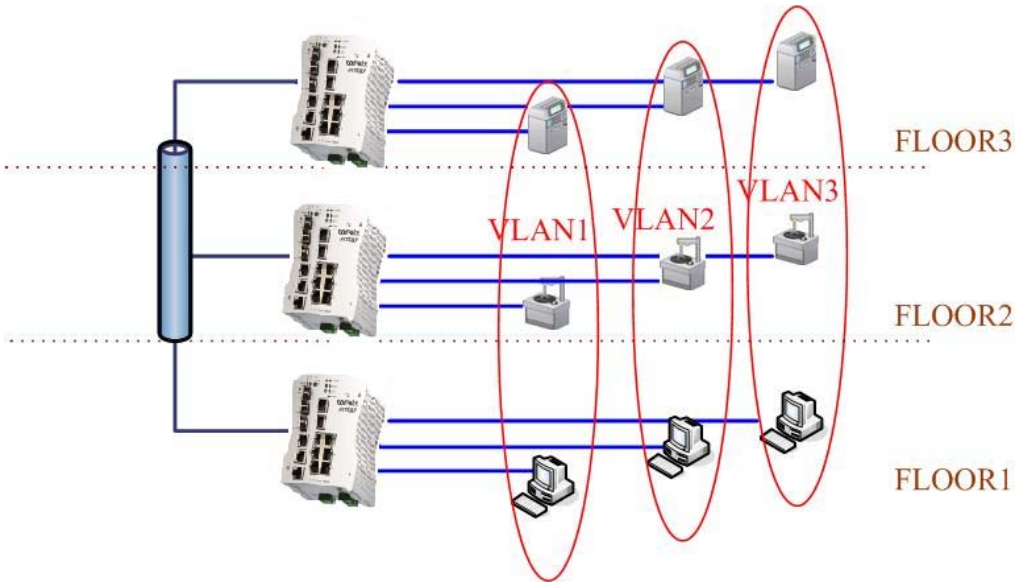
	fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Root Information	Switch# show spanning-tree mst root MST Instance Root Address Root Priority Root Cost Root Port Max age Hello Fwd dly -------- -------------- -------- ---------- ------ ----- ----- ----- MST00 0012.77ee.eeee 32768 0 N/A 20 2 15 MST01 0012.77ee.eeee 32768 0 N/A 20 2 15 MST02 0012.77ee.eeee 32768 0 N/A 20 2 15
MSTP Instance Information	Switch# show spanning-tree mst 1 ###### MST01 vlans mapped: 2 Bridge address 0012.77ee.eeee priority 32768 (sysid 1) Root this switch for MST01 Port Role State Cost Prio.Nbr Type ------ ---------- ---------- -------- ---------- ---------- fa1 Designated Forwarding 200000 128.1 P2P Internal(MSTP) fa2 Designated Forwarding 200000 128.2 P2P Internal(MSTP)
MSTP Port Information	Switch# show spanning-tree mst interface fa1 Interface fastethernet1 of MST00 is Designated Forwarding Edge Port : Edge (Edge) BPDU Filter : Disabled Link Type : Auto (Point-to-point) BPDU Guard : Disabled Boundary : Internal(MSTP) BPDUs : sent 6352, received 0 Instance Role State Cost Prio.Nbr Vlans mapped -------- ---------- ---------- -------- ---------- ---------- 0 Designated Forwarding 200000 128.1 1,4-4094 1 Designated Forwarding 200000 128.1 2 2 Designated Forwarding 200000 128.1 3
Multiple Super Ring	
Create or configure a Ring	Switch(config)# multiple-super-ring 1 Ring 1 created Switch(config-multiple-super-ring)# ***Note: 1 is the target Ring ID which is going to be created or configured.***
Super Ring Version	Switch(config-multiple-super-ring)# version any-ring any ring auto detection default set default to rapid super ring rapid-super-ring rapid super ring super-ring super ring Switch(config-multiple-super-ring)# version rapid-super-ring
Priority	Switch(config-multiple-super-ring)# priority <0-255> valid range is 0 to 255 default set default Switch(config)# super-ring priority 100
Ring Port	Switch(config-multiple-super-ring)# port IFLIST Interface list, ex: fa1,fa3-5,gi8-10 cost path cost Switch(config-multiple-super-ring)# port fa1,fa2
Ring Port Cost	Switch(config-multiple-super-ring)# port cost <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255 Switch(config-multiple-super-ring)# port cost 100 <0-255> valid range is 0 or 255 default set default (128)valid range is 0 or 255

	Switch(config-super-ring-plus)# port cost 100 200 Set path cost success.
Rapid Dual Homing	Switch(config-multiple-super-ring)# rapid-dual-homing enable Switch(config-multiple-super-ring)# rapid-dual-homing disable Switch(config-multiple-super-ring)# rapid-dual-homing port IFLIST Interface name, ex: fastethernet1 or gi8 auto-detect up link auto detection IFNAME Interface name, ex: fastethernet1 or gi8 Switch(config-multiple-super-ring)# rapid-dual-homing port fa3,fa5-6 set Rapid Dual Homing port success. Note: auto-detect is recommended for dual Homing..
Ring Info	
Ring Info	Switch# show multiple-super-ring [Ring ID] [Ring1] Ring1 Current Status : Disabled Role : Disabled Ring Status : Abnormal Ring Manager : 0000.0000.0000 Blocking Port : N/A Giga Copper : N/A Configuration : Version : Rapid Super Ring Priority : 128 Ring Port : fa1, fa2 Path Cost : 100, 200 Dual-Homing II : Disabled Statistics : Watchdog sent 0, received 0, missed 0 Link Up sent 0, received 0 Link Down sent 0, received 0 Role Transition count 0 Ring State Transition count 1 Ring ID is optional. If the ring ID is typed, this command will only display the information of the target Ring.

4.6 VLAN

A Virtual LAN (VLAN) is a “logical” grouping of nodes for the purpose of limiting a broadcast domain to specific members of a group without physically grouping the members together. That means, VLAN allows you to isolate network traffic so that only members of VLAN could receive traffic from the same VLAN members. Basically, creating a VLAN from a switch is the logical equivalent of physically reconnecting a group of network devices to another Layer 2 switch, without actually disconnecting these devices from their original switches.

PMI Industrial Ethernet Switch supports 802.1Q VLAN. 802.1Q VLAN is also known as Tag-Based VLAN. This Tag-Based VLAN allows VLAN to be created across different switches. IEEE 802.1Q tag-based VLAN makes use of VLAN control information stored in a VLAN header attached to IEEE 802.3 packet frames. This tag contains a VLAN Identifier (VID) that indicates which VLAN a frame belongs to. Since each switch only has to check a frame’s tag, without the need to dissect the contents of the frame, this also saves a lot of computing resources within the switch.



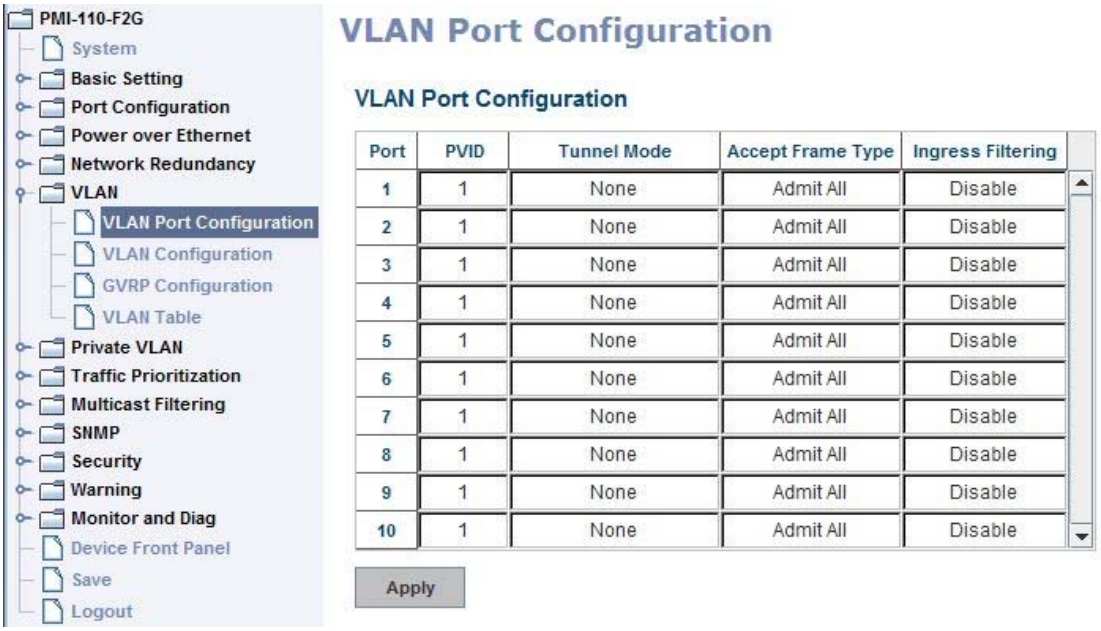
VLAN Configuration group enables you to Add/Remove VLAN, configure port Ingress/Egress parameters and view VLAN table.

Following commands are included in this group:

4.6.1 VLAN Port Configuration
4.6.2 VLAN Configuration
4.6.3 GVRP Configuration
4.6.4 VLAN Table
4.6.5 CLI Commands of the VLAN

4.6.1 VLAN Port Configuration

VLAN Port Configuration allows you to set up VLAN port parameters to specific port. These parameters include PVID, Accept Frame Type and Ingress Filtering.



PVID: The abbreviation of the **Port VLAN ID**. Enter port VLAN ID here. PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs.

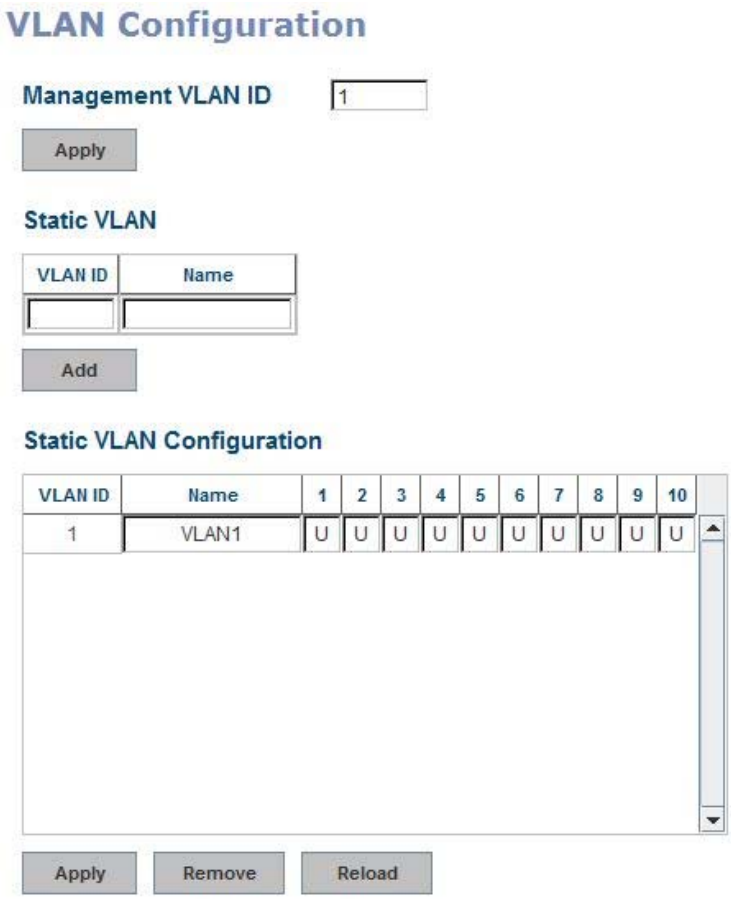
The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. You can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column. Type the PVID you'd like to configure here.

Accept Frame Type: This column defines the accepted frame type of the port. There are 2 modes you can select, **Admit All** and **Tag Only**. Admit All mode means that the port can accept both tagged and untagged packets. Tag Only mode means that the port can only accept tagged packets.

Ingress Filtering: Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN they claimed or not. Then the port determines if the frames can be processed or not. For example, if a tagged frame from Engineer VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Engineer VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped.

4.6.2 VLAN Configuration

In this page, you can assign Management VLAN, create the static VLAN, and assign the Egress rule for the member ports of the VLAN.



Management VLAN ID: The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch. The default management VLAN ID is **1**.

Static VLAN: You can assign a VLAN ID and VLAN Name for new VLAN here.

VLAN ID is used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094. 1 is the default VLAN.

VLAN Name is a reference for network administrator to identify different VLANs. The available character is 12 for you to input. If you don't input VLAN name, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID).

The steps to create a new VLAN: Type in VLAN ID and NAME, and press **Add** to create a new VLAN. Then you can see the new VLAN in the Static VLAN

After created the VLAN, the status of the VLAN will remain in Unused until you add ports to the VLAN.

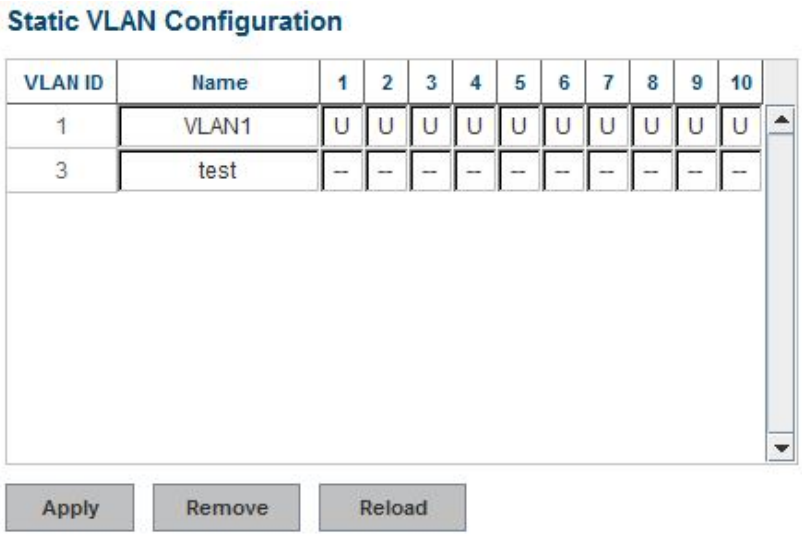
Note: *Before you change the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can't access the switch via the network.*

Note: *Currently PMI6710G only support max 256 groups VLAN.*

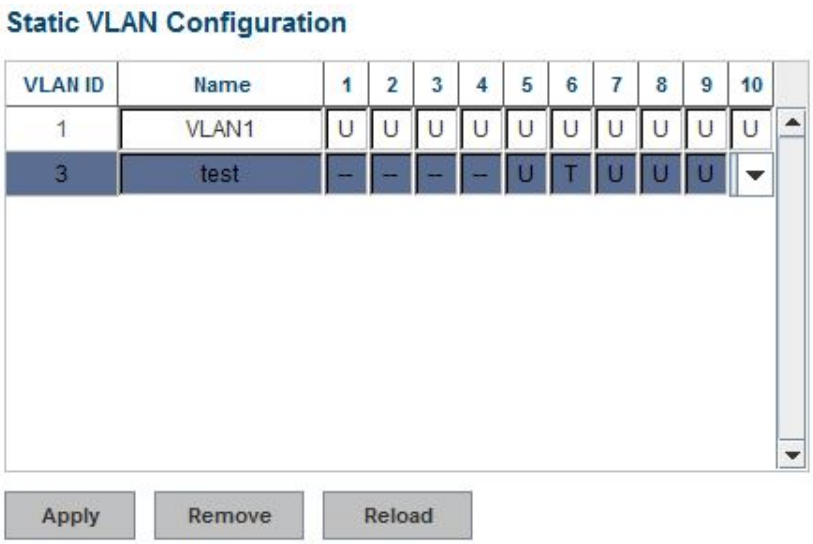
Static VLAN Configuration

You can see the created VLANs and specify the egress (outgoing) port rule to be **Untagged or Tagged** here.

Static VLAN Configuration table. You can see that new VLAN 3 is created. VLAN name is test. Egress rules of the ports are not configured now.



Configure Egress rule of the ports.



-- : Not available

U: **Untag**: Indicates that egress/outgoing frames are not VLAN tagged.

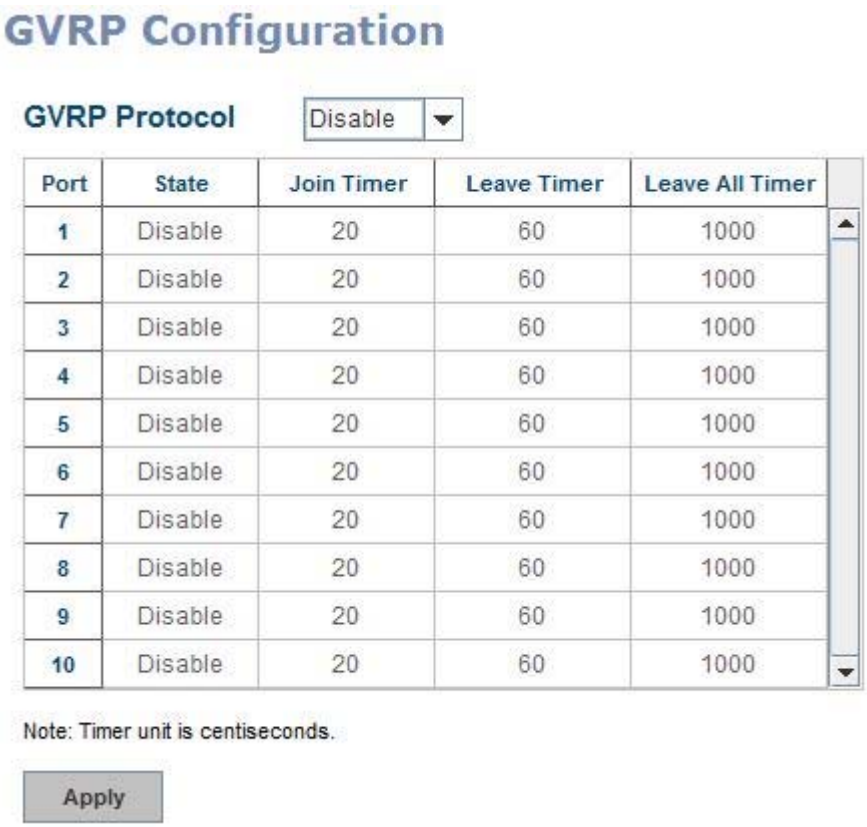
T : **Tag**: Indicates that egress/outgoing frames are to be VLAN tagged.

Steps to configure Egress rules: Select the VLAN ID. Entry of the selected VLAN turns to light blue. Assign Egress rule of the ports to **U** or **T**. Press **Apply** to apply the

setting. If you want to remove one VLAN, select the VLAN entry. Then press **Remove** button.

4.6.3 GVRP configuration

GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network.



GVRP Protocol: Allow user to enable/disable GVRP globally.
State: After enable GVRP globally, here still can enable/disable GVRP by port.
Join Timer: Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis
Leave Timer: Control the time to release the GVRP reservation after received the GVRP Leave BPDU. An instance of the timer is required for each state machine that is in the LV state
Leave All Timer: Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-Port, per-GARP Participant basis

4.6.4 VLAN Table

This table shows you current settings of your VLAN table, including VLAN ID, Name, Status, and Egress rule of the ports.

VLAN ID: ID of the VLAN.

Name: Name of the VLAN.

Status: Static shows this is a manually configured static VLAN. **Unused** means this VLAN is created by UI/CLI and has no member ports. This VLAN is not workable yet. **Dynamic** means this VLAN is learnt by GVRP.

After created the VLAN, the status of this VLAN will remain in unused status until you add ports to the VLAN.

4.6.5 CLI Commands of the VLAN

Command Lines of the VLAN port configuration, VLAN configuration and VLAN table display

Feature	Command Line
VLAN Port Configuration	
VLAN Port PVID	Switch(config-if)# switchport trunk native vlan 2 Set port default vlan id to 2 success
Port Accept Frame Type	Switch(config)# inter fa1 Switch(config-if)# acceptable frame type all any kind of frame type is accepted! Switch(config-if)# acceptable frame type vlantaggedonly only vlan-tag frame is accepted!
Ingress Filtering (for fast Ethernet port 1)	Switch(config)# interface fa1 Switch(config-if)# ingress filtering enable ingress filtering enable Switch(config-if)# ingress filtering disable ingress filtering disable
Egress rule – Untagged (for VLAN 2)	Switch(config-if)# switchport access vlan 2 switchport access vlan - success
Egress rule – Tagged (for	Switch(config-if)# switchport trunk allowed vlan add 2

VLAN 2)	
Display – Port Ingress Rule (PVID, Ingress Filtering, Acceptable Frame Type)	Switch# show interface fa1 Interface fastethernet1 Administrative Status : Enable Operating Status : Not Connected Duplex : Auto Speed : Auto Flow Control :off Default Port VLAN ID: 2 Ingress Filtering : Disabled Acceptable Frame Type : All Port Security : Disabled Auto Negotiation : Enable Loopback Mode : None STP Status: disabled Default CoS Value for untagged packets is 0. Mdix mode is Auto. Medium mode is Copper.
Display – Port Egress Rule (Egress rule, IP address, status)	Switch# show running-config …… ! interface fastethernet1 switchport access vlan 1 switchport access vlan 3 switchport trunk native vlan 2 ……. interface vlan1 ip address 192.168.2.8/24 no shutdown
VLAN Configuration	
Create VLAN (2)	Switch(config)# vlan 2 vlan 2 success Switch(config)# interface vlan 2 Switch(config-if)# *Note: In CLI configuration, you should create a VLAN interface first. Then you can start to add/remove ports. Default status of the created VLAN is unused until you add member ports to it.*
Remove VLAN	Switch(config)# no vlan 2 no vlan success *Note: You can only remove the VLAN when the VLAN is in unused mode.*
VLAN Name	Switch(config)# vlan 2 vlan 2 has exists Switch(config-vlan)# name v2 Switch(config-vlan)# no name *Note: Use no name to change the name to default name, VLAN VID.*
VLAN description	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# description this is the VLAN 2

	Switch(config-if)# no description ->Delete the description.
IP address of the VLAN	Switch(config)# interface vlan 2 Switch(config-if)# Switch(config-if)# ip address 192.168.2.18/24 Switch(config-if)# no ip address 192.168.2.8/24 ->Delete the IP address
Create multiple VLANs (VLAN 5-10)	Switch(config)# interface vlan 5-10
Shut down VLAN	Switch(config)# interface vlan 2 Switch(config-if)# shutdown Switch(config-if)# no shutdown ->Turn on the VLAN
Display – VLAN table	Switch# sh vlan VLAN Name Status Trunk Ports Access Ports ---- ---------- ------- ---------- ---------- 1 VLAN1 Static - fa1-7,gi8-10 2 VLAN2 Unused - - 3 test Static fa4-7,gi8-10 fa1-3,fa7,gi8-10
Display – VLAN interface information	Switch# show interface vlan1 interface vlan1 is up, line protocol detection is disabled index 14 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST> HWaddr: 00:07:7C:ff:01:b0 inet 192.168.2.100/24 broadcast 192.168.2.255 input packets 639, bytes 38248, dropped 0, multicast packets 0 input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0 output packets 959, bytes 829280, dropped 0 output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0 collisions 0
GVRP configuration	
GVRP enable/disable	Switch(config)# gvrp mode disable Disable GVRP feature globally on the switch enable Enable GVRP feature globally on the switch Switch(config)# gvrp mode enable Gvrp is enabled on the switch!
Configure GVRP timer Join timer /Leave timer/ LeaveAll timer	Switch(config)# inter fa1 Switch(config-if)# garp timer <10-10000> Switch(config-if)# garp timer 20 60 1000 Note: The unit of these timer is centisecond
Management VLAN	
Management VLAN	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# no shutdown
Display	Switch# show running-config .... ! interface vlan1 ip address 192.168.2.17/24 ip igmp no shutdown ! ....

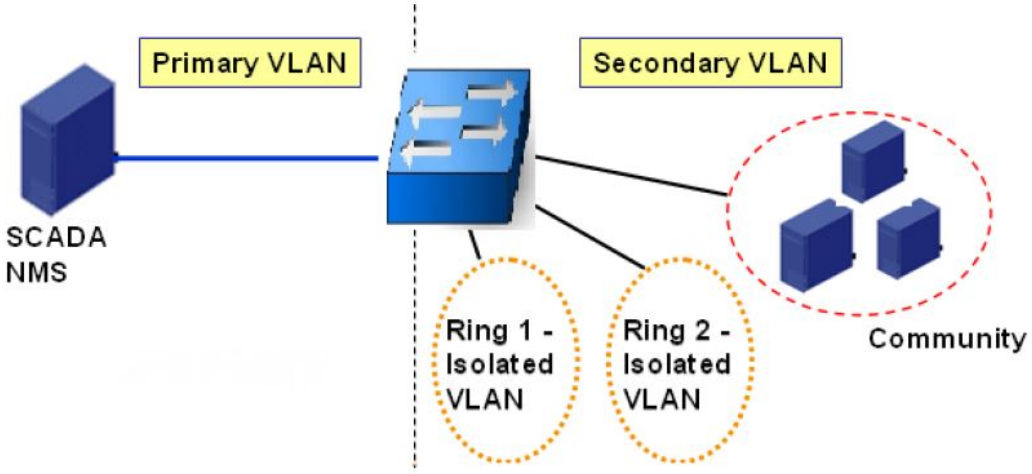
4.7 Private VLAN

The private VLAN helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. The Private VLAN provides primary and secondary VLAN within a single switch.

Primary VLAN: The uplink port is usually the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with lower Secondary VLANs.

Secondary VLAN: The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN. The client ports can be isolated VLANs or can be grouped in the same Community VLAN. The ports within the same community VLAN can communicate with each other. However, the isolated VLAN ports can Not.

The figure shows the typical Private VLAN network. The SCADA/Public Server or NMS workstation is usually located in primary VLAN. The clients PCs or Rings are located within Secondary.



Private VLAN (PVLAN) Configuration group enables you to Configure PVLAN, PVLAN Port and see the PVLAN Information.

Following commands are included in this group:

4.7.1 PVLAN Configuration

4.7.2 PVLAN Port Configuration

4.7.3 CLI Commands of the PVLAN

4.7.1 PVLAN Configuration

PVLAN Configuration allows you to assign Private VLAN type. After created VLAN in VLAN Configuraiton page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN you want configure.

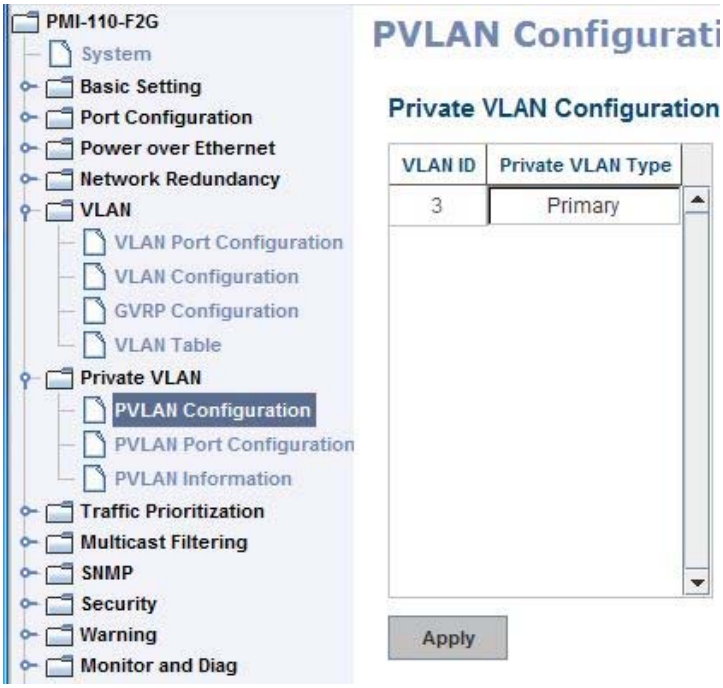
None: The VLAN is Not included in Private VLAN.

Primary: The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.

Isolated: The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated.

Community: The VLAN is the Community VLAN. The member ports of the VLAN

can communicate with each other.



4.7.2 PVLAN Port Configuration

PVLAN Port Configuration page allows configure Port Configuration and Private VLAN Association.

Private VLAN Association (PVLAN)

Secondary VLAN: After the Isolated and Community VLAN Type is assigned in Private VLAN Configuration page, the VLANs are belonged to the Secondary VLAN and displayed here.

Primary VLAN: After the Primary VLAN Type is assigned in Private VLAN Configuration page, the secondary VLAN can associate to the Primary VLAN ID. Select the Primary VLAN ID here.

Note: Before configuring PVLAN port type, the Private VLAN Association should be done first.

Port Configuraion

PVLAN Port Type :

Normal: The Normal port is None PVLAN ports, it remains its original VLAN setting.

Host: The Host type ports can be mapped to the Secondary VLAN.

Promiscuous: The promiscuous port can be associated to the Primary VLAN.

VLAN ID: After assigned the port type, the web UI display the available VLAN ID the port can associate to.

For example:

1. VLAN Create: VLAN 2-5 are created in VLAN Configuration page.

2. Private VLAN Type: VLAN 2-5 has its Private VLAN Type configured in Private VLAN Configuration page.

VLAN 2 is belonged to Primary VLAN.

VLAN 3-5 are belonged to secondary VLAN (Isolated or Community).

3. Private VLAN Association: Associate VLAN 3-5 to VLAN 2 in Private VLAN Association first.

4. Private VLAN Port Configuraiton

VLAN 2 – Primary -> The member port of VLAN 2 is promiscuous port.

VLAN 3 – Isolated -> The Host port can be mapped to VLAN 3.

VLAN 4 – Community -> The Host port can be mapped to VLAN 3.

VLAN 5 – Community -> The Host port can be mapped to VLAN 3.

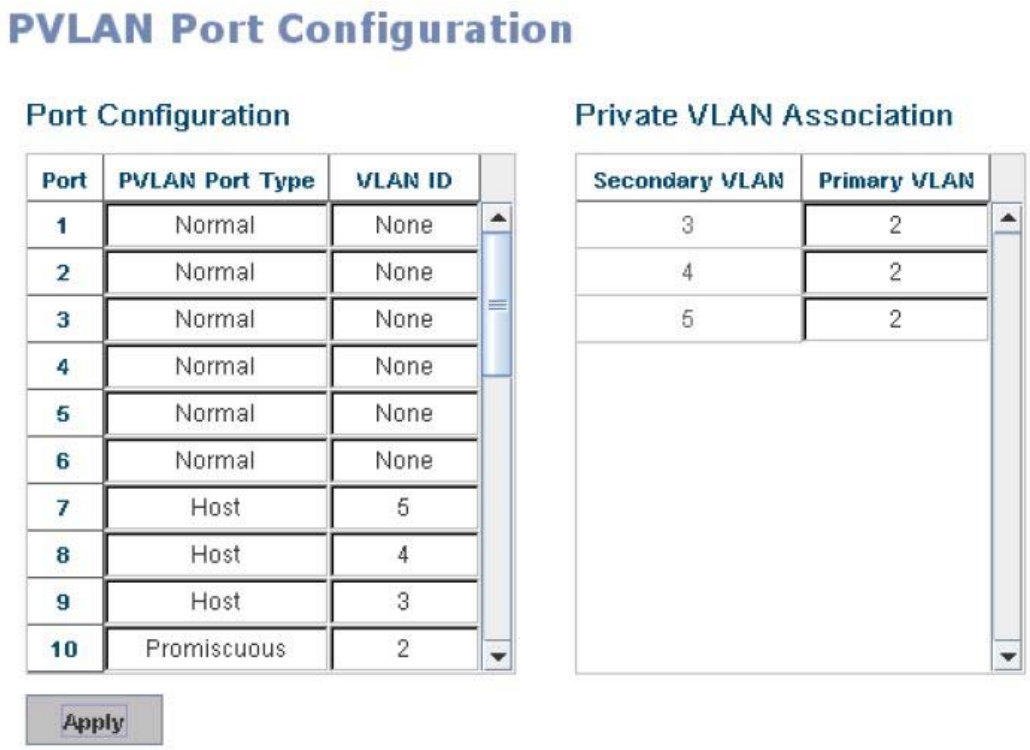
5. Result:

VLAN 2 -> VLAN 3, 4, 5; member ports can communicate with ports in secondary VLAN.

VLAN 3 -> VLAN 2, member ports are isolated, but it can communicate with member port of VLAN 2..

VLAN 4 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.

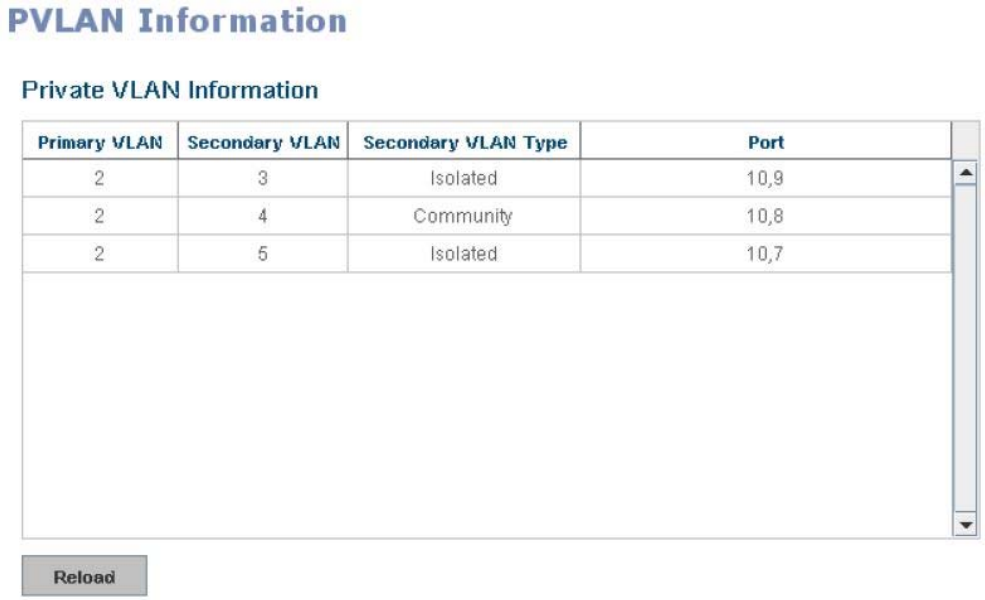
VLAN 5 -> VLAN 2, member ports within the community can communicate with each other and communicate with member port of VLAN 2.



4.7.3 Private VLAN Information

This page allows you to see the Private VLAN information.

4.7.4 CLI Command of the PVLAN



Command Lines of the Private VLAN configuration

Feature	Command Line
Private VLAN Configuration	
Create VLAN	Switch(config)# vlan 2 vlan 2 success Switch(config-vlan)# end End current mode and change to enable mode exit Exit current mode and down to previous mode list Print command list name Assign a name to vlan no no private-vlan Configure a private VLAN
Private VLAN Type Choose the Types Primary Type Isolated Type Community Type	**Go to the VLAN you want configure first.** Switch(config)# vlan (VID) Switch(config-vlan)# private-vlan community Configure the VLAN as an community private VLAN isolated Configure the VLAN as an isolated private VLAN primary Configure the VLAN as a primary private VLAN Switch(config-vlan)# private-vlan primary <cr> Switch(config-vlan)# private-vlan isolated <cr> Switch(config-vlan)# private-vlan community <cr>

Private VLAN Port Configuraiton	
Go to the port configuraiton	Switch(config)# interface (port_number, ex: gi9) Switch(config-if)# switchport private-vlan host-association Set the private VLAN host association mapping map primary VLAN to secondary VLAN
Private VLAN Port Type Promiscuous Port Type Host Port Type	Switch(config-if)# switchport mode private-vlan Set private-vlan mode Switch(config-if)# switchport mode private-vlan host Set the mode to private-vlan host promiscuous Set the mode to private-vlan promiscuous Switch(config-if)# switchport mode private-vlan promiscuous <cr> Switch(config-if)# switchport mode private-vlan host <cr>
Private VLAN Port Configuration PVLAN Port Type Host Association primary to secondary (The command is only available for host port.)	Switch(config)# interface gi9 Switch(config-if)# switchport mode private-vlan host Switch(config-if)# switchport private-vlan host-association <2-4094> Primary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 <2-4094> Secondary range VLAN ID of the private VLAN port association Switch(config-if)# switchport private-vlan host-association 2 3
Mapping primary to secondary VLANs (This command is only available for promiscuous port)	Switch(config)# interface gi10 Switch(config-if)# switchport mode private-vlan promiscuous Switch(config-if)# switchport private-vlan mapping 2 add 3 Switch(config-if)# switchport private-vlan mapping 2 add 4 Switch(config-if)# switchport private-vlan mapping 2 add 5
Private VLAN Information	
Private VLAN Information	Switch# show vlan private-vlan FLAGS: I -> Isolated P -> Promiscuous C -> Community Primary Secondary Type Ports ------- --------- ----------------- ---------------------- 2 3 Isolated gi10(P),gi9(I) 2 4 Community gi10(P),gi8(C) 2 5 Community gi10(P),fa7(C),gi9(I) 10 - - -
PVLAN Type	Switch# show vlan private-vlan type Vlan Type Ports ---- ----------------- ----------------- 2 primary gi10 3 isolated gi9 4 community gi8 5 community fa7,gi9 10 primary -

Host List	Switch# show vlan private-vlan port-list Ports Mode Vlan ----- ---------- ---- 1 normal - 2 normal - 3 normal - 4 normal - 5 normal - 6 normal - 7 host 5 8 host 4 9 host 3 10 promiscuous 2
Running Config Information

	switchport private-vlan mapping 2 add 3-5 …… ……..

4.8 Traffic Prioritization

Quality of Service (QoS) provides traffic prioritization mechanism which allows users to deliver better service to certain flows. QoS can also help to alleviate congestion problems and ensure high-priority traffic is delivered first. This section allows you to configure Traffic Prioritization settings for each port with regard to setting priorities.

PMI QOS supports 4 physical queues, weighted fair queuing (WRR) and Strict Priority scheme, which follows 802.1p COS tag and IPv4 TOS/DiffServ information to prioritize the traffic of your industrial network.

Following commands are included in this group:

4.8.1 QoS Setting

4.8.2 CoS-Queue Mapping

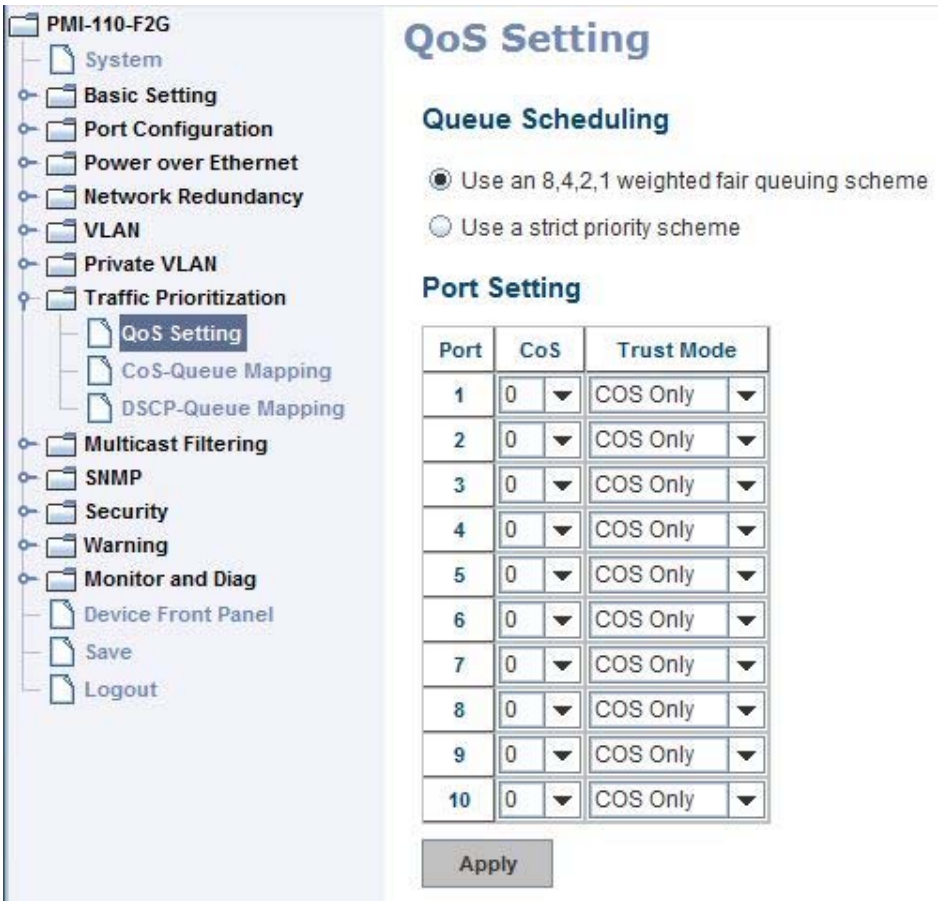
4.8.3 DSCP-Queue Mapping

4.8.4 CLI Commands of the Traffic Prioritization

4.8.1 QoS Setting

Queue Scheduling

You can select the Queue Scheduling rule as follows:



Use an 8,4,2,1 weighted fair queuing scheme. This is also known as **WRR** (Weight Round Robin)**.** PMI will follow 8:4:2:1 rate to process the packets in a queue from the highest priority to the lowest. For example, the system will process 8 packets with the highest priority in the queue, 4 with middle priority, 2 with low priority, and 1 with the lowest priority at the same time.

Use a strict priority scheme. Packets with higher priority in the queue will always be processed first, except that there is no packet with higher priority.

Port Setting

CoS column is to indicate default port priority value for untagged or priority-tagged frames. When PMI receives the frames, PMI will attach the value to the CoS field of the incoming VLAN-tagged packets. You can enable

0,1,2,3,4,5,6 or 7 to the port.

Trust Mode is to indicate Queue Mapping types for you to select.

COS Only: Port priority will only follow COS-Queue Mapping you have assigned.

DSCP Only: Port priority will only follow DSCP-Queue Mapping you have assigned.

COS first: Port priority will follow COS-Queue Mapping first, and then DSCP-Queue Mapping rule.

DSCP first: Port priority will follow DSCP-Queue Mapping first, and then COS-Queue Mapping rule.

Default priority type is **COS Only**. The system will provide default COS-Queue table to which you can refer for the next command.

After configuration, press **Apply** to enable the settings.

4.8.2 CoS-Queue Mapping

This page is to change CoS values to Physical Queue mapping table. Since the switch fabric of PMI only supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map CoS value to the level of the physical queue.

In PMI, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Westermo uses 802.p suggestion as default values. You can find CoS values 1 and 2 are mapped to physical Queue 0, the lowest queue. CoS values 0 and 3 are mapped to physical Queue 1, the low/normal physical queue. CoS values 4 and 5 are mapped to physical Queue 2, the middle physical queue. CoS values 6 and 7 are mapped to physical Queue 3, the high physical queue.

CoS-Queue Mapping
CoS-Queue Mapping
CoS 0 1 2 3 4 5 6 7
Queue 1 0 0 1 2 2 3 3
Note: Queue 3 is the highest priority queue in using Strict Priority scheme.
Apply

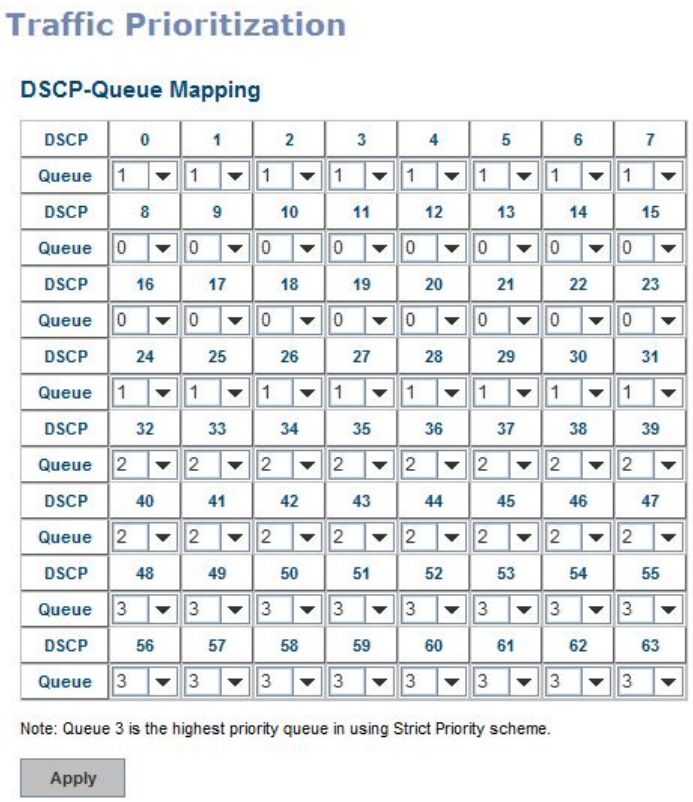
After configuration, press **Apply** to enable the settings.

4.8.3 DSCP-Queue Mapping

This page is to change DSCP values to Physical Queue mapping table. Since the switch fabric of PMI only supports 4 physical queues, Lowest, Low, Middle and High. Users should therefore assign how to map DSCP value to the level of the physical queue. In PMI, users can freely change the mapping table to follow the

upper layer 3 switch or routers' DSCP setting.

After configuration, press **Apply** to enable the settings.



4.8.4 CLI Commands of the Traffic Prioritization

Command Lines of the Traffic Prioritization configuration

Feature	Command Line
QoS Setting	
Queue Scheduling – Strict Priority	Switch(config)# qos queue-sched sp Strict Priority wrr Weighted Round Robin (Use an 8,4,2,1 weight) Switch(config)# qos queue-sched sp <cr>
Queue Scheduling - WRR	Switch(config)# qos queue-sched wrr
Port Setting – CoS (Default Port Priority)	Switch(config)# interface **fa1** Switch(config-if)# qos cos DEFAULT-COS Assign an priority (7 highest) Switch(config-if)# qos cos 7 The default port CoS value is set 7 ok. ***Note: When change the port setting, you should Select the specific port first. Ex: fa1 means fast Ethernet port 1.***
Port Setting – Trust Mode- CoS Only	Switch(config)# interface fa1 Switch(config-if)# qos trust cos

	The port trust is set CoS only ok.
Port Setting – Trust Mode- CoS First	Switch(config)# interface fa1 Switch(config-if)# qos trust cos-first The port trust is set CoS first ok.
Port Setting – Trust Mode- DSCP Only	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp The port trust is set DSCP only ok.
Port Setting – Trust Mode- DSCP First	Switch(config)# interface fa1 Switch(config-if)# qos trust dscp-first The port trust is set DSCP first ok.
Display – Queue Scheduling	Switch# show qos queue-sched QoS queue scheduling scheme : Weighted Round Robin (Use an 8,4,2,1 weight)
Display – Port Setting - Trust Mode	Switch# show qos trust QoS Port Trust Mode : Port Trust Mode -----+------------ 1 DSCP first 2 COS only 3 COS only 4 COS only 5 COS only 6 COS only 7 COS only 8 COS only 9 COS only 10 COS only
Display – Port Setting – CoS (Port Default Priority)	Switch# show qos port-cos Port Default Cos : Port CoS -----+---- 1 7 2 0 3 0 4 0 5 0 6 0 7 0 8 0 9 0 10 0
CoS-Queue Mapping	
Format	Switch(config)# qos cos-map PRIORITY Assign an priority (7 highest) Switch(config)# qos cos-map 1 QUEUE Assign an queue (0-3) ***Note: Format: qos cos-map priority_value queue_value***
Map CoS 0 to Queue 1	Switch(config)# qos cos-map 0 1 The CoS to queue mapping is set ok.
Map CoS 1 to Queue 0	Switch(config)# qos cos-map 1 0 The CoS to queue mapping is set ok.
Map CoS 2 to Queue 0	Switch(config)# qos cos-map 2 0 The CoS to queue mapping is set ok.
Map CoS 3 to Queue 1	Switch(config)# qos cos-map 3 1 The CoS to queue mapping is set ok.

Map CoS 4 to Queue 2	Switch(config)# qos cos-map 4 2 The CoS to queue mapping is set ok.
Map CoS 5 to Queue 2	Switch(config)# qos cos-map 5 2 The CoS to queue mapping is set ok.
Map CoS 6 to Queue 3	Switch(config)# qos cos-map 6 3 The CoS to queue mapping is set ok.
Map CoS 7 to Queue 3	Switch(config)# qos cos-map 7 3 The CoS to queue mapping is set ok.
Display – CoS-Queue mapping	Switch# sh qos cos-map CoS to Queue Mapping : CoS Queue ---- + ------ 0 1 1 0 2 0 3 1 4 2 5 2 6 3 7 3
DSCP-Queue Mapping	
Format	Switch(config)# qos dscp-map PRIORITY Assign an priority (63 highest) Switch(config)# qos dscp-map 0 QUEUE Assign an queue (0-3) ***Format: qos dscp-map priority_value queue_value***
Map DSCP 0 to Queue 1	Switch(config)# qos dscp-map 0 1 The TOS/DSCP to queue mapping is set ok.
Display – DSCO-Queue mapping	Switch# show qos dscp-map DSCP to Queue Mapping : (dscp = d1 d2) d2| 0 1 2 3 4 5 6 7 8 9 d1 | -----+---------- 0 | 1 1 1 1 1 1 1 1 0 0 1 | 0 0 0 0 0 0 0 0 0 0 2 | 0 0 0 0 1 1 1 1 1 1 3 | 1 1 2 2 2 2 2 2 2 2 4 | 2 2 2 2 2 2 2 2 3 3 5 | 3 3 3 3 3 3 3 3 3 3 6 | 3 3 3 3

4.9 Multicast Filtering

For multicast filtering, PMI Switch uses IGMP Snooping technology. IGMP (Internet Group Management Protocol) is an Internet Protocol that provides a way for internet device to report its multicast group membership to adjacent routers. Multicasting allows one computer on the internet to send data to a multitude of other computers that have identified themselves as being interested in receiving the originating computers data.

Multicasting is useful for such applications as updating the address books of mobile computer users in the field, sending out newsletters to a distribution list, and broadcasting streaming media to an audience that has tuned into the event by setting up multicast group membership.

In effect, IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

Message	Description
Query	A message sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group.
Report	A message sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message.
Leave Group	A message sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group.

You can enable **IGMP Snooping** and **IGMP Query** functions here. You will see the information of the IGMP Snooping function in this section, including different multicast groups' VID and member ports, and IP multicast addresses that range from 224.0.0.0 to 239.255.255.255.

In this section, Force filtering can determined whether the switch flooding unknown multicast or not.

Following commands are included in this group:

4.9.1 IGMP Snooping

4.9.2 IGMP Query

4.9.3 Force Filtering

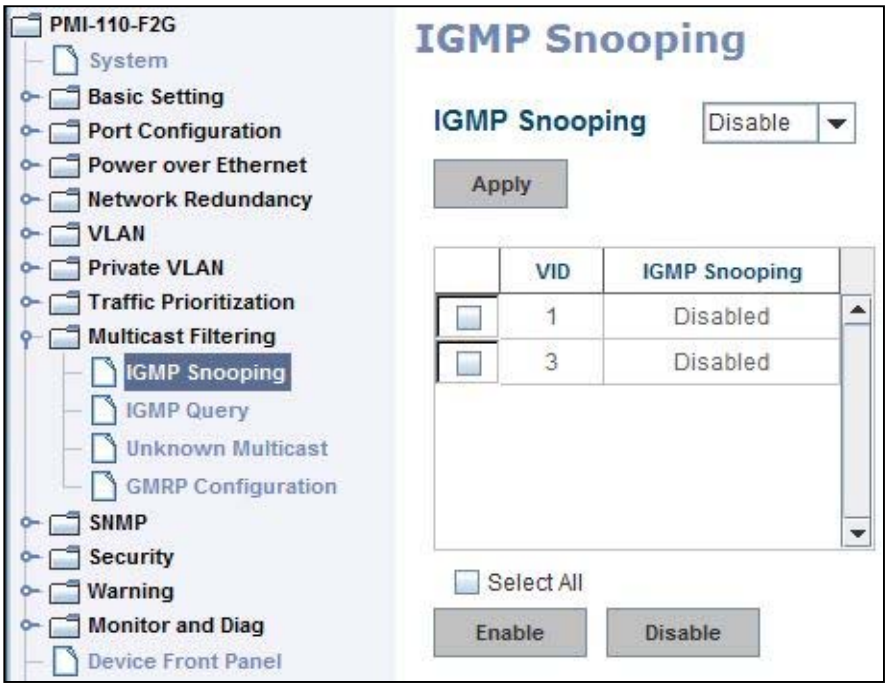
4.9.4 CLI Commands of the Multicast Filtering

4.9.1 IGMP Snooping

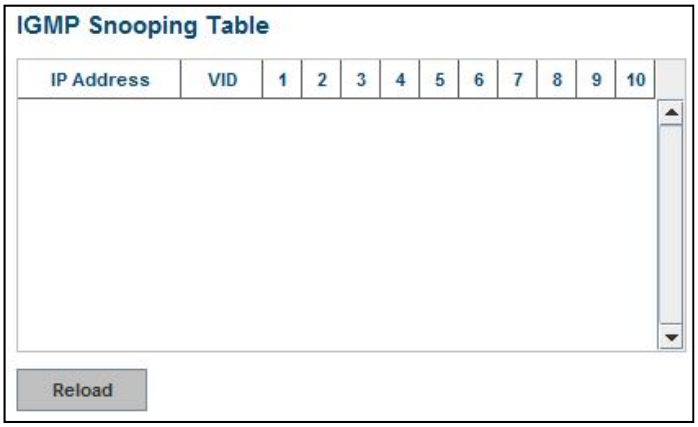
This page is to enable IGMP Snooping feature, assign IGMP Snooping for specific VLAN, and view IGMP Snooping table from dynamic learnt or static manual key-in. PMI Switch support IGMP snooping V1/V2/V3 automatically and IGMP query V1/V2.

IGMP Snooping, you can select **Enable** or **Disable** here. After enabling IGMP Snooping, you can then enable IGMP Snooping for specific VLAN. You can enable IGMP Snooping for some VLANs so that some of the VLANs will support IGMP Snooping and others won't.

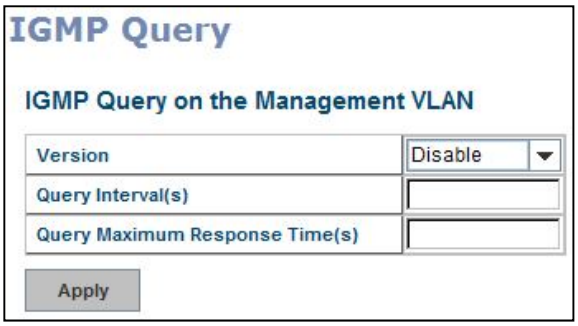
To assign IGMP Snooping to VLAN, please select the **checkbox** of VLAN ID or select **Select All** checkbox for all VLANs. Then press **Enable**. In the same way, you can also **Disable** IGMP Snooping for certain VLANs.



IGMP Snooping Table: In the table, you can see multicast group IP address, VLAN ID it belongs to, and member ports of the multicast group. PMI Managed Switch series supports 256 multicast groups. Click on **Reload** to refresh the table.



4.9.2 IGMP Query



This page allows users to configure **IGMP Query** feature. Since PMI Switch can only be configured by member ports of the management VLAN, IGMP Query can only be enabled on the management VLAN. If you want to run IGMP Snooping feature in several VLANs, you should notice that whether each VLAN has its own IGMP Querier first.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it. For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

In IGMP Query selection, you can select V1, V2 or Disable. **V1** means IGMP V1 General Query and **V2** means IGMP V2 General Query. The query will be forwarded to all multicast groups in the VLAN. **Disable** allows you to disable IGMP Query.

Query Interval(s): The period of query sent by querier.

Query Maximum Response Time: The span querier detect to confirm there are no more directly connected group members on a LAN.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.9.3 Force Filtering

The Force filtering function allows the switch to filter the unknown-multicast data flow. If Force filtering is enabled, all the unknown multicast data will be discarded.

4.9.4 CLI Commands of the Multicast Filtering

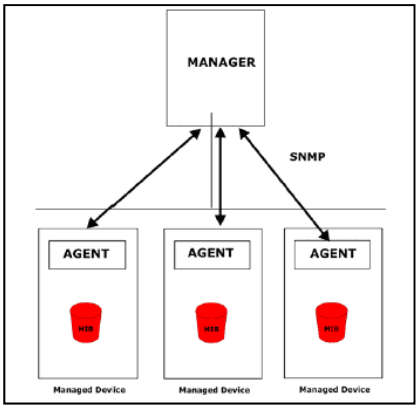
Command Lines of the multicast filtering configuration

Feature	Command Line
IGMP Snooping	

IGMP Snooping - Global	Switch(config)# ip igmp snooping IGMP snooping is enabled globally. Please specify on which vlans IGMP snooping enables
IGMP Snooping - VLAN	Switch(config)# ip igmp snooping vlan VLANLIST allowed vlan list all all existed vlan Switch(config)# ip igmp snooping vlan 1-2 IGMP snooping is enabled on VLAN 1-2.
Disable IGMP Snooping - Global	Switch(config)# no ip igmp snoopin IGMP snooping is disabled globally ok.
Disable IGMP Snooping - VLAN	Switch(config)# no ip igmp snooping vlan 3 IGMP snooping is disabled on VLAN 3.
Display – IGMP Snooping Setting	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv1 query-interval; 125s query-max-response-time: 10s Switch# sh ip igmp snooping IGMP snooping is globally enabled Vlan1 is IGMP snooping enabled Vlan2 is IGMP snooping enabled Vlan3 is IGMP snooping disabled
Display – IGMP Table	Switch# sh ip igmp snooping multicast all VLAN IP Address Type Ports ---- --------------- ------- ------------------------- 1 239.192.8.0 IGMP fa6, 1 239.255.255.250 IGMP fa6,
IGMP Query	
IGMP Query V1	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp v1
IGMP Query V2	Switch(config)# int vlan 1 (Go to management VLAN) Switch(config-if)# ip igmp
IGMP Query version	Switch(config-if)# ip igmp version 1 Switch(config-if)# ip igmp version 2
Disable	Switch(config)# int vlan 1 Switch(config-if)# no ip igmp
Display	Switch# sh ip igmp interface vlan1 enabled: Yes version: IGMPv2 query-interval: 125s query-max-response-time: 10s Switch# show running-config .... ! interface vlan1 ip address 192.168.2.200/24 ip igmp no shutdown ! .....

Force filtering	
Enable Force filtering	Switch(config)# mac-address-table multicast filtering Filtering unknown multicast addresses ok!
Disable Force filtering	Switch(config)# no mac-address-table multicast filtering Flooding unknown multicast addresses ok!

4.10 SNMP



Simple Network Management Protocol (SNMP) is a protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. PMI Manageed Switch support SNMP v1 and v2c and V3.

An SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

Following commands are included in this group:

4.10.1 SNMP Configuration

4.10.2 SNMPv3 Profile

4.10.3 SNMP Traps

4.10.4 SNMP CLI Commands for SNMP

4.10.1 SNMP Configuration

This page allows users to configure SNMP V1/V2c Community. The community string can be viewed as the password because SNMP V1/V2c doesn't request you to enter password before you try to access SNMP agent.

The community includes 2 privileges, Read Only and Read and Write.

With **Read Only** privilege, you only have the ability to read the values of MIB tables. Default community string is Public.

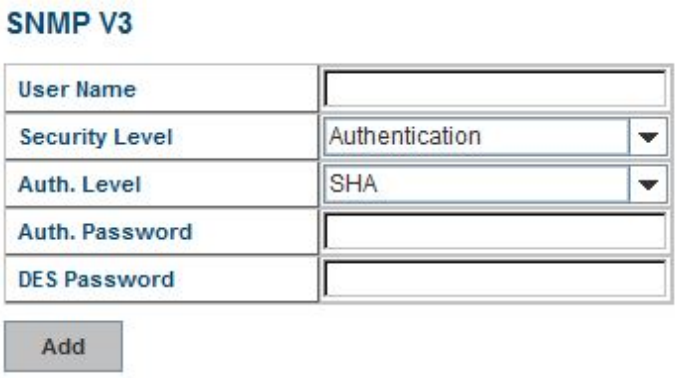
With **Read and Write** privilege, you have the ability to read and set the values of MIB tables. Default community string is Private.

PMI Managed Switch allows users to assign 4 community strings. Type the community string and select the privilege. Then press **Apply**.

Note: *When you first install the device in your network, we highly recommend you to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.*

4.10.2 SNMP V3 Profile

SNMP v3 can provide more security functions when the user performs remote management through SNMP protocol. It delivers SNMP information to the administrator with user authentication; all of data between *PMI Switch* and the administrator are encrypted to ensure secure communication.



Security Level: Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy.

Authentication Protocol: Here the user can select either MD5 (Message-Digest algorithm 5) or SHA (Secure Hash Algorithm). MD5 is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. *PMI Managed Switch* provides 2 user authentication protocols in MD5 and SHA. You will need to configure SNMP v3 parameters for your SNMP tool with the same authentication method.

Authentication Password: Here the user enters the SNMP v3 user authentication

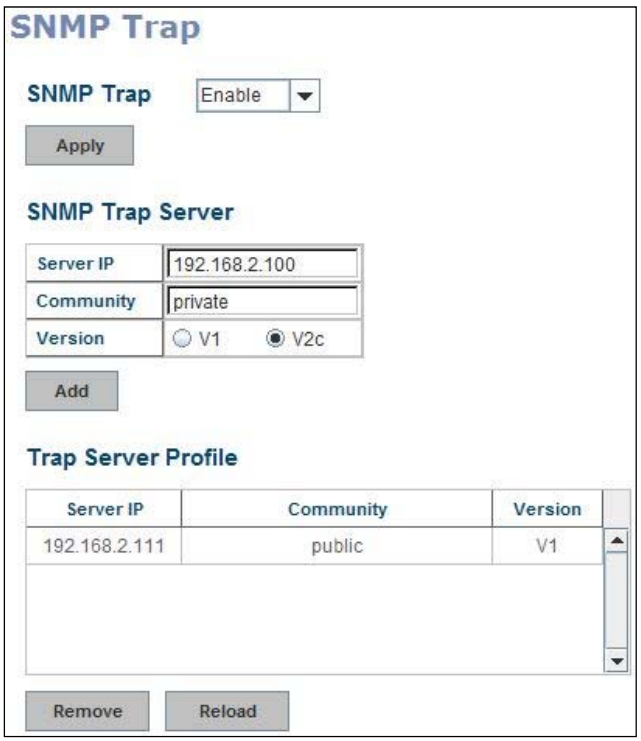
password.

DES Encryption Password: Here the user enters the password for SNMP v3 user DES Encryption.

4.10.3 SNMP Traps

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap information. So you don't need to install new application to read the notification information.

This page allows users to **Enable SNMP Trap,** configure the **SNMP Trap server IP**, **Community** name, and trap **Version V1 or V2**. After configuration, you can see the change of the SNMP pre-defined standard traps and Westermo pre-defined traps. The pre-defined traps can be found in Westermo private MIB, that included in the CD-manual or download from Westermo Web-site.



4.10.4 CLI Commands of the SNMP

Command Lines of the SNMP configuration

Feature	Command Line
SNMP Community	
Read Only Community	Switch(config)# snmp-server community public ro community string add ok
Read Write Community	Switch(config)# snmp-server community private rw community string add ok
SNMP Trap	
Enable Trap	Switch(config)# snmp-server enable trap Set SNMP trap enable ok.
SNMP Trap Server IP without specific community name	Switch(config)# snmp-server host 192.168.2.33 SNMP trap host add OK.
SNMP Trap Server IP with version 1 and community	Switch(config)# snmp-server host 192.168.2.33 version 1 private SNMP trap host add OK. ***Note: private is the community name, version 1 is the SNMP version***
SNMP Trap Server IP with version 2 and community	Switch(config)# snmp-server host 192.168.2.33 version 2 private SNMP trap host add OK.
Disable SNMP Trap	Switch(config)# no snmp-server enable trap Set SNMP trap disable ok.
Display	Switch# sh snmp-server trap SNMP trap: Enabled SNMP trap community: public Switch# show running-config ..... snmp-server community public ro snmp-server community private rw snmp-server enable trap snmp-server host 192.168.2.33 version 2 admin snmp-server host 192.168.2.33 version 1 admin ……..

4.11 Security

PMI Switch provides several security features for you to secure your connection. The features include Port Security and IP Security.

Following commands are included in this group:

4.11.1 Port Security

4.11.2 IP Security

4.11.3 IEEE 802.1x

4.11.4 CLI Commands of the Security

4.11.1 Port Security

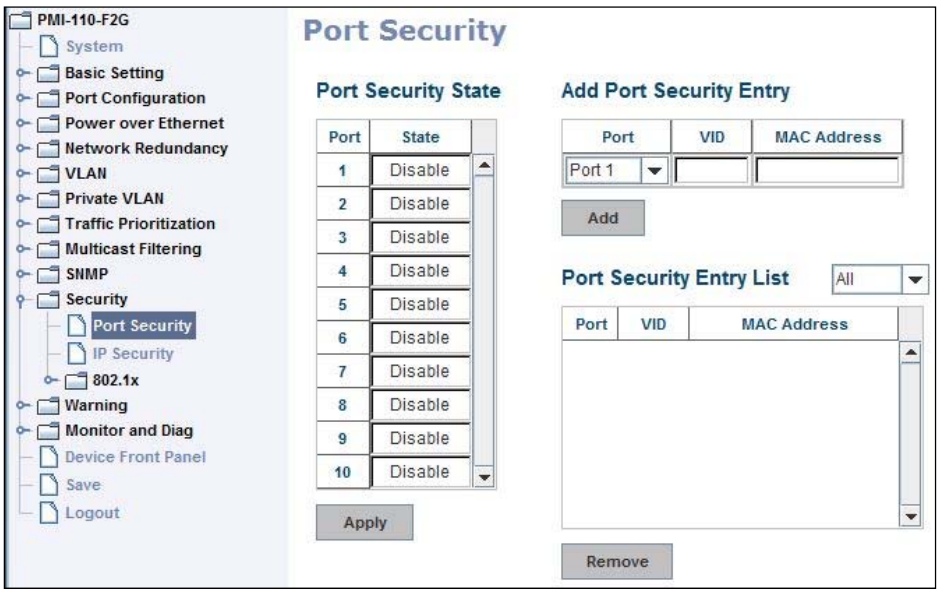
Port Security feature allows you to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in Port Security List can access the switch and transmit/receive traffic. This is a simple way to secure your network environment and not to be accessed by hackers.

This page allows you to enable Port Security and configure Port Security entry.

Port Security State: Change Port Security State of the port to Enable first.

Add Port Security Entry: Select the port, and type VID and MAC address. Format of the MAC address is xxxx.xxxx.xxxx. Ex: 0012.7701.0101. Max volume of one port is 10. So the system can accept 100 Port Security MAC addresses in total.

Port Security List: This table shows you those enabled port security entries. You can click on **Remove** to delete the entry.



Once you finish configuring the settings, click on **Apply / Add** to apply your configuration.

4.11.2 IP Security

In IP Security section, you can set up specific IP addresses to grant authorization for management access to this PMI via a web browser or Telnet.

IP Security: Select Enable and **Apply** to enable IP security function.

Add Security IP: You can assign specific IP addresses, and then press **Add**. Only these IP addresses can access and manage PMI via a web browser or Telnet. Max security IP is 10.

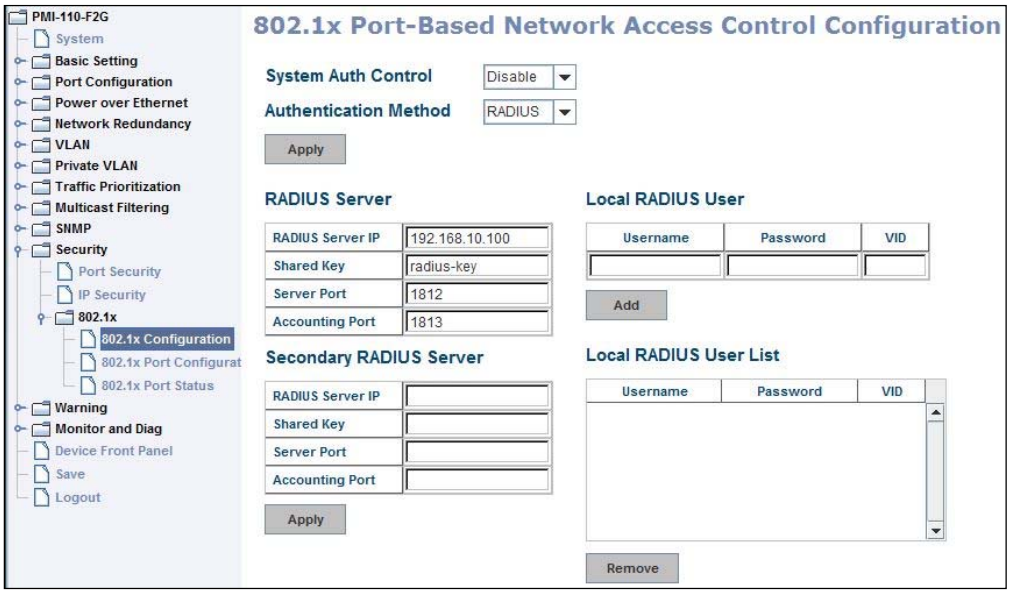
Security IP List: This table shows you added security IP addresses. You can press **Remove** to delete, **Reload** to reload the table.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.11.3 IEEE 802.1x

4.11.3.1 802.1X configuration

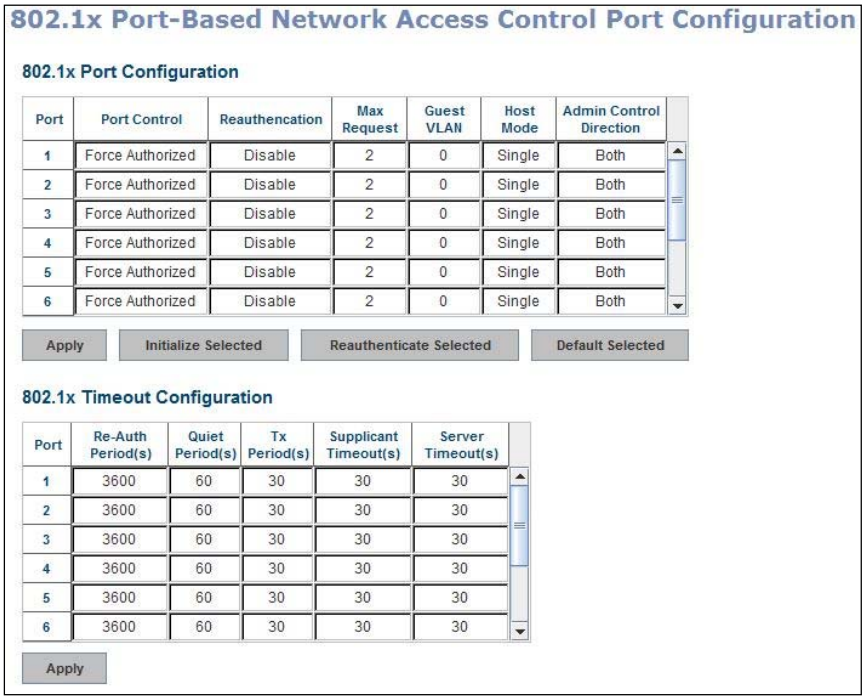
IEEE 802.1X is the protocol that performing authentication to obtain access to IEEE 802 LANs. It is port-base network access control. With the function, PMI Switch could control which connection is available or not.



System AuthControl: To enable or disable the 802.1x authentication.
Authentication Method: Radius is a authentication server that provide key for authentication, with this method, user must connect switch to server. If user select Local for the authentication method, switch use the local user data base which can be create in this page for authentication.
Radius Server IP: The IP address of Radius server
Shared Key: it is the password for communicate between switch and Radius Server.
Server Port: UDP port of Radius server.
Accounting Port: Port for packets that contain the information of account login or logout.
Secondary Radius Server IP: Secondary Radius Server could be set in case of the primary radius server down.
802.1X Local User: Here User can add Account/Password for local authentication.
802.1X Local user List: This is a list shows the account information, User also can remove selected account Here.

4.11.3.2 802.1x Port Configuration

After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.



Port control: Force Authorized means this port is authorized; the data is free to in/out. Force unauthorized just opposite, the port is blocked. If users want to control this port with Radius Server, please select Auto for port control.

Reauthentication: If enable this field, switch will ask client to re-authenticate. The default time interval is 3600 seconds.

Max Request: the maximum times that the switch allow client request.

Guest VLAN: 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to Guest VLAN.

Host Mode: if there are more than one device connected to this port, set the Host Mode to single means only the first PC authenticate success can access this port. If this port is set to multi, all the device can access this port once any one of them pass the authentication.

Control Direction: determined devices can end data out only or both send and receive.

Re-Auth Period: control the Re-authentication time interval, 1~65535 is available.

Quiet Period: When authentication failed, Switch will wait for a period and try to communicate with radius server again.

Tx period: the time interval of authentication request.

Supplicant Timeout: the timeout for the client authenticating

Sever Timeout: The timeout for server response for authenticating.

Once you finish configuring the settings, click on **Apply** to apply your configuration.

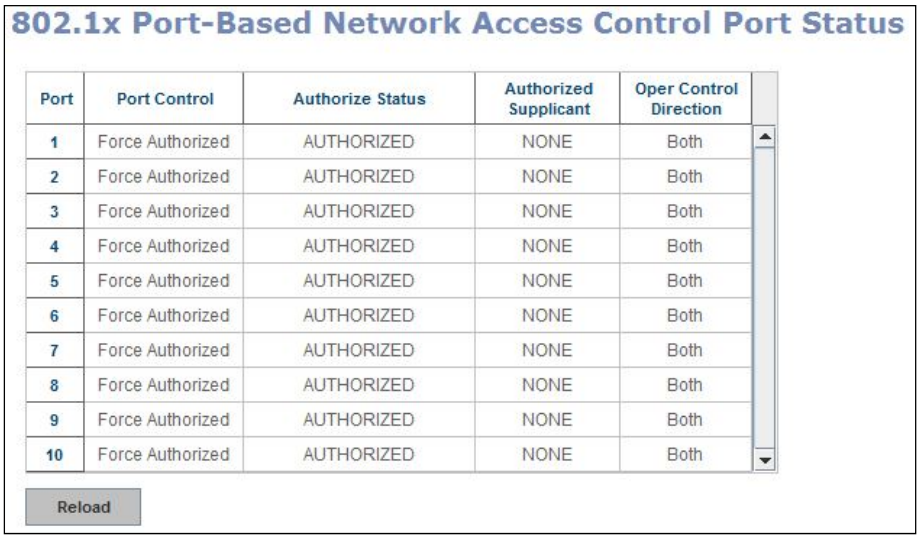
Click **Initialize Selected** to set the authorize state of selected port to initialize status.

Click **Reauthenticate Selected** to send EAP Request to supplicant to request reauthentication.

Click **Default Selected** to reset the configurable 802.1x parameters of selected port to the default values.

4.11.3.3 802.1X Port Status

Here user can observe the port status for Port control status, Authorize Status, Authorized Supplicant and Oper Control Direction each port.


802.1x Port-Based Network Access Control Port Status
Port
Port Control
Authorize Status
Authorized Supplicant
Oper Control Direction
1 Force Authorized AUTHORIZED NONE Both
2 Force Authorized AUTHORIZED NONE Both
3 Force Authorized AUTHORIZED NONE Both
4 Force Authorized AUTHORIZED NONE Both
5 Force Authorized AUTHORIZED NONE Both
6 Force Authorized AUTHORIZED NONE Both
7 Force Authorized AUTHORIZED NONE Both
8 Force Authorized AUTHORIZED NONE Both
9 Force Authorized AUTHORIZED NONE Both
10 Force Authorized AUTHORIZED NONE Both
Reload

4.11.4 CLI Commands of the Security

Command Lines of the Security configuration

Feature	Command Line
Port Security	
Add MAC	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fa1 mac-address-table unicast static set ok!
Port Security	Switch(config)# interface fa1 Switch(config-if)# switchport port-security Disables new MAC addresses learning and aging activities! ***Note: Rule: Add the static MAC, VLAN and Port binding first, then enable the port security to stop new MAC learning.***
Disable Port Security	Switch(config-if)# no switchport port-security Enable new MAC addresses learning and aging activities!
Display	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ---------- ---------- ------- ---------- 0012.7701.0101 Static 1 fa1
IP Security	
IP Security	Switch(config)# ip security Set ip security enable ok. Switch(config)# ip security host 192.168.2.200 Add ip security host 192.168.2.200 ok.
Display	Switch# show ip security ip security is enabled ip security host: 192.168.2.200
802.1x	
enable diable	Switch(config)# dot1x system-auth-control Switch(config)# Switch(config)# no dot1x system-auth-control Switch(config)#
authentic-method	Switch(config)# dot1x authentic-method local Use the local username database for authentication radius Use the Remote Authentication Dial-In User Service (RADIUS) servers for authentication Switch(config)# dot1x authentic-method radius Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.2.200 key 1234 RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.2.200 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius server-ip	Switch(config)# dot1x radius Switch(config)# dot1x radius server-ip 192.168.2.200 key 1234

	RADIUS Server Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) RADIUS Server IP : 192.168.2.120 RADIUS Server Key : 1234 RADIUS Server Port : 1812 RADIUS Accounting Port : 1813 Switch(config)#
radius secondary-server-ip	Switch(config)# dot1x radius secondary-server-ip 192.168.2.250 key 5678 Port number NOT given. (default=1812) RADIUS Accounting Port number NOT given. (default=1813) Secondary RADIUS Server IP : 192.168.2.250 Secondary RADIUS Server Key : 5678 Secondary RADIUS Server Port : 1812 Secondary RADIUS Accounting Port : 1813
User name/password for authentication	Switch(config)# dot1x username Westermo passwd Westermo vlan 1

4.12 Warning

PMI Switch provides several types of Warning features for you to remote monitor the status of end devices or the change of your network. The features include Fault Relay, System Log and SMTP E-mail Alert.

Following commands are included in this group:

4.12.1 Fault Relay

4.12.2 Event & E-mail warning

4.12.2.1 Event Selection

4.12.2.2 Syslog configuration

4.12.2.2 SMTP Configuration

4.12.3 CLI Commands

4.12.1 Fault Relay

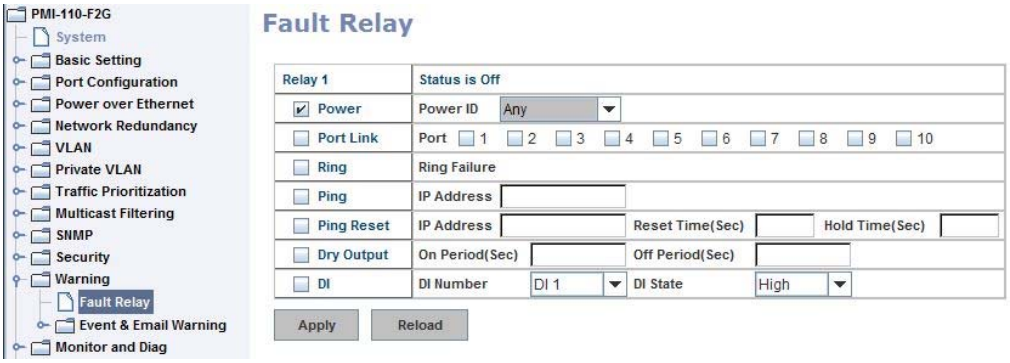
The PMI Switch provides 1 alarm relay output, also known as Digital Output. The relay (DO) contact is energized from normal and will form a close circuit under system fault conditions.The fault conditions include power failure, Ethernet port link fault, Ring topology change, Ping Failure, DI state change or ping remote IP address failure.

From the firmware version 1.1a, the fault relay supports multiple event relay binding function. That means fault realy not only support one event only, it can be assigned multiple event. The condition or term described as following table.

Term	conditction	description
Power	Power DC1 Power DC2 Any	Detect power input status. If one of condiction occurred, relay triggered.
Port Link	Port number	Monitoring port link down event
Ring	Ring failure	If ring topology changed
Ping	**IP Address:** remote device's IP address.	If target IP does not reply ping request, then relay active.
Ping Reset	**IP address:** remote device's address **Reset Time**: duration of output open. **Hodl Time:** duration of Ping hold time.	Ping target device and trigger relay to emulate power reset for remote device, if remote system crash. Note: once perform Ping reset, the relay output will form a short circuit.
Dry Output	**On period:** duration of relay output short (close). **Off period**: duration of relay output open.	Relay continuous perform On/Off behavior with different duration.
DI	DI number	Relay trigger when DI states change to Hi or

	(PMI-110-F2GG supports 1 DI)	Low

The Fault relay configuration UI has shown as below:



The relay supports multiple event trigger function; click and select type of evnt and setting the detail information, and then click the icon “Apply” to activte the replay alarm function.

Relay 1: Show current relay state. If the relay is triggered, the event type will be marked with the symbol- ∗. On the upper diagram, the replay is triggerd by power event – Any.

Power: relay trigger by power down event. It can be set to minotoring power DC1, DC2 and Any.

Port Link: monitoring the port link status.

Ring: monitoring the ring status.

Ping: ping predefined IP address. If the deivce does not reply the Ping, the relay will be triggered.

Ping Reset: the relay active as a power switch for remote device. If the relay alarm function is occupied for the Ping Reset, the other event should be disabled. It may cause the relay wrong action.

IP address: device’s IPaddress whose power wiring is connected with relay output.

Reset Time: user defined duration of relay contact open to emulate power switch off. After the duration, the relay contact will change to close to emulates power switch on.

Hold time: user defined the booting time that deivce needed. After relay contact close, the Switch will start ping after count down the hold time.

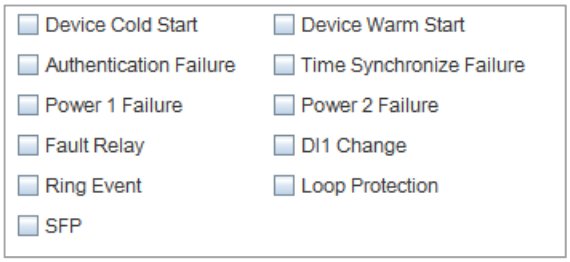
Dry Output: dorced the relay active as a on/off switch. This function also should not apply with other event.

On period /Off period: the duration of relay on and off. The available range of a period is 0-65535 seconds

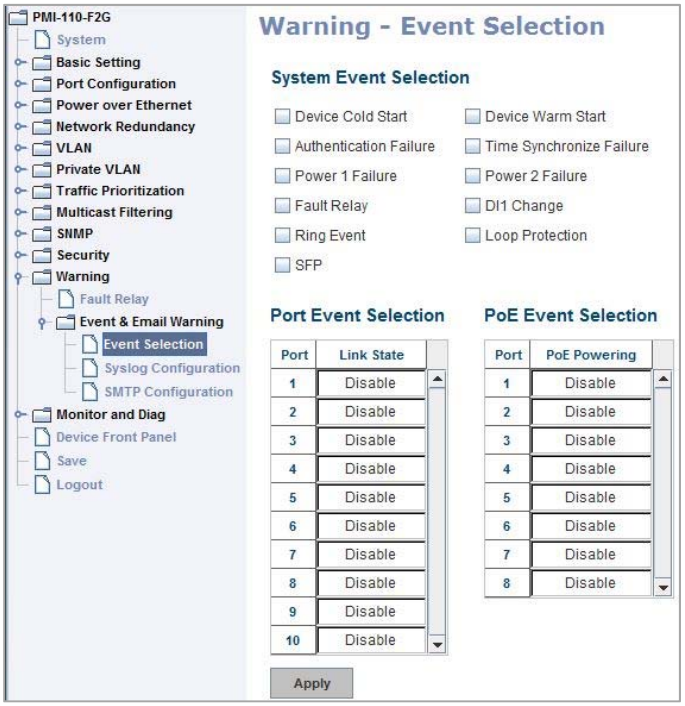
DI: monitoring the Digital input state.

4.12.2.1 Event & E-mail Warning – Event Selection

Event Types can be divided into two basic groups: System Events and Port Events. System Events are related to the overall function of the switch, whereas Port Events related to the activity of specific ports



Once you finish configuring the settings, click on **Apply** to apply your configuration.



System Event Selection	**Warning Event is sent when…..**
Device Cold Start	Power is cut off and then reconnected.
Device Warm Start	Reboot the device by CLI or Web UI.
Authentication failure	An incorrect password, SNMP Community String is entered.
Time Synchronize Failure	Accessing to NTP Server is failure.
Power 1/ 2 Failure	The power input is failure.
Fault Relay	The DO/Fault Relay is on.
Ring Topology Changes	Master of Super Ring has changed or backup path is activated.
SFP	The SFP transceiver's state is abnormal.
Port Event Selection	**Warning Event is sent when…..**
Link-Up	The port is connected to another device
Link-Down	The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down)
Both	The link status changed.
PoE Event Selection	**Warning Event is sent when…..**
Diable	Port PoE function is disabled
Enable	Port PoE function is enabled.

4.12.2.2 SysLog Configuration

System Log is useful to provide system administrator locally or remotely monitor switch events history. There are 2 System Log modes provided by PMI Switch, local mode and remote mode.

Local Mode: In this mode, PMI Switch will print the occurred events selected in the Event Selection page to System Log table of PMI Switch. You can monitor the system logs in [Monitor and Diag] / [Event Log] page.

Remote Mode: The remote mode is also known as Server mode in PMI managed switch series. In this mode, you should assign the IP address of the System Log server. PMI Switch will send the occurred events selected in Event Selection page to System Log server you assigned.

Both: Above 2 modes can be enabled at the same time.

Warning - SysLog configuration
Syslog Mode
Disable
Remote IP Address
Note: When enabled Local and Both mode, you can monitor the system logs in the [Monitor and Diag]/[Event Log] page.
Apply

Once you finish configuring the settings, click on **Apply** to apply your configuration.

Note: *When enabling Local or Both modes, you can monitor the system logs in [Monitor and Diag] / [Event Log] page.*

4.12.2.3 SMTP Configuration

PMI Switch supports E-mail Warning feature. The switch will send the occurred events to remote E-mail server. The receiver can then receive notification by E-mail. The E-mail warning is conformed to SMTP standard.

This page allows you to enable E-mail Alert, assign the SMTP Server IP, Sender E-mail, and Receiver E-mail. If SMTP server requests you to authorize first, you can also set up the username and password in this page.

Field	Description
SMTP Server IP Address	Enter the IP address of the email Server
Authentication	Click on check box to enable password
User Name	Enter email Account name (Max.40 characters)
Password	Enter the password of the email account
Confirm Password	Re-type the password of the email account
You can set up to 4 email addresses to receive email alarm from PMI	
Rcpt E-mail Address 1	The first email address to receive email alert from PMI (Max. 40 characters)
Rcpt E-mail Address 2	The second email address to receive email alert from PMI (Max. 40 characters)
Rcpt E-mail Address 3	The third email address to receive email alert from PMI (Max. 40 characters)
Rcpt E-mail Address 4	The fourth email address to receive email alert from PMI (Max. 40 characters)

Once you finish configuring the settings, click on **Apply** to apply your configuration.

4.12.3 CLI Commands

Command Lines of the Warning configuration

Feature	Command Line
Relay Output	
Relay Output	Switch(config)# relay 1 di DI state dry dry output ping ping failure port port link failure power power failure ring super ring failure ***Note: Select Relay 1 or 2 first, then select the event types.***
DI State	Switch(config)# relay 1 di <1-2> DI number Switch(config)# relay 1 di 1 high high is abnormal low low is abnormal Switch(config)# relay 1 di 1 high
Dry Output	Switch(config)# relay 1 dry <0-4294967295> turn on period in second Switch(config)# relay 1 dry 5 <0-4294967295> turn off period in second Switch(config)# relay 1 dry 5 5
Ping Failure	Switch(config)# relay 1 ping 192.168.2.200 <cr> reset reset a device Switch(config)# relay 1 ping 192.168.2. 200 reset <1-65535> reset time Switch(config)# relay 1 ping 192.168.2. 200 reset 60 <0-65535> hold time to retry Switch(config)# relay 1 ping 192.168.2. 200 reset 60 60
Port Link Failure	Switch(config)# relay 1 port PORTLIST port list Switch(config)# relay 1 port fa1-5
Power Failure	Switch(config)# relay 1 power <1-2> power id Switch(config)# relay 1 power 1 Switch(config)# relay 1 power 2
Super Ring Failure	Switch(config)# relay 1 ring
Disable Relay	Switch(config)# no relay <1-2> relay id Switch(config)# no relay 1 *(Relay_ID: 1 or 2)* <cr>
Display	Switch# show relay 1 Relay Output Type : Port Link Port : 1, 2, 3, 4, Switch# show relay 2 Relay Output Type : Super Ring
Event Selection	
Event Selection	Switch(config)# warning-event coldstart Switch cold start event warmstart Switch warm start event linkdown Switch link down event

	linkup Switch link up event all Switch all event authentication Authentication failure event di Switch di event fault-relay Switch fault relay event power Switch power failure event sfp-ddm Switch SFP DDM abnormal event super-ring Switch super ring topology change event time-sync Switch time synchronize event
Ex: Cold Start event	Switch(config)# warning-event coldstart Set cold start event enable ok.
Ex: Link Up event	Switch(config)# warning-event linkup [IFNAME] Interface name, ex: fastethernet1 or gi8 Switch(config)# warning-event linkup fa5 Set fa5 link up event enable ok.
Display	Switch# show warning-event Warning Event: Cold Start: Enabled Warm Start: Disabled Authentication Failure: Disabled Link Down: fa4-5 Link Up: fa4-5 Power Failure: Super Ring Topology Change: Disabled Fault Relay: Disabled Time synchronize Failure: Disable SFP DDM: Enabled DI:DI1
Syslog Configuration	
Local Mode	Switch(config)# log syslog local
Server Mode	Switch(config)# log syslog remote 192.168.2.200
Both	Switch(config)# log syslog local Switch(config)# log syslog remote 192.168.2. 200
Disable	Switch(config)# no log syslog local
SMTP Configuration	
SMTP Enable	Switch(config)# smtp-server enable email-alert SMTP Email Alert set enable ok.
Sender mail	Switch(config)# smtp-server server 192.168.2. 200 ACCOUNT SMTP server mail account, ex: support@westermo.se Switch(config)# smtp-server server 192.168.2. 200 support@westermo.se SMTP Email Alert set Server: 192.168.2. 200, Account: support@westermo.se ok.
Receiver mail	Switch(config)# smtp-server receipt 1 support@westermo.se SMTP Email Alert set receipt 1: support@westermo.se ok.
Authentication with username and password	Switch(config)# smtp-server authentication username admin password westermo SMTP Email Alert set authentication Username: admin, Password: westermo ***Note: You can assign string to username and password.***
Disable SMTP	Switch(config)# no smtp-server enable email-alert SMTP Email Alert set disable ok.
Disable Authentication	Switch(config)# no smtp-server authentication SMTP Email Alert set Authentication disable ok.
Dispaly	Switch# sh smtp-server SMTP Email Alert is Enabled

	Server: 192.168.2.200, Account: support@westermo.se Authentication: Enabled Username: admin, Password: westermo SMTP Email Alert Receipt: Receipt 1: support@westermo.se Receipt 2: Receipt 3: Receipt 4:

4.13 Monitor and Diag

PMI Switch provides several types of features for you to monitor the status of the switch or diagnostic for you to check the problem when encountering problems related to the switch. The features include MAC Address Table, Port Statistics, Port Mirror, Event Log and Ping.

Following commands are included in this group:

4.13.1 MAC Address Table

4.13.2 Port Statistics

4.13.3 Port Mirror

4.13.4 Event Log

4.13.5 Topology Discovery

4.13.6 Ping

4.13.7 CLI Commands of the Monitor and Diag

4.13.1 MAC Address Table

PMI-110-F2G provides 8K entries in MAC Address Table. In this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click on **Apply** to change the value.

Aging Time (Sec)

Each switch fabric has limit size to write the learnt MAC address. To save more entries for new MAC address, the switch fabric will age out non-used MAC address entry per Aging Time timeout. The default Aging Time is 300 seconds. The Aging Time can be modified in this page.

Static Unicast MAC Address

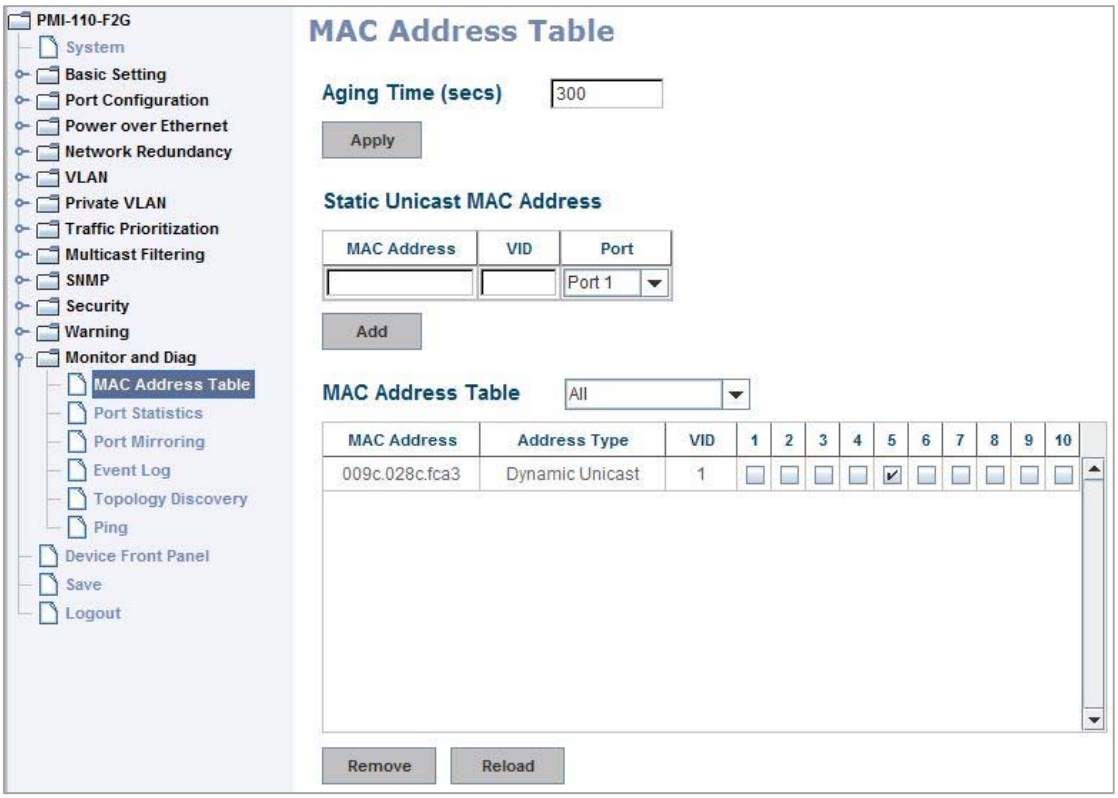
In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, you can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.

MAC Address Table

In this MAC Address Table, you can see all the MAC Addresses learnt by the switch fabric. The packet types include Management Unicast, Static Unicast, Dynamic Unicast, Static Multicast and Dynamic Multicast. The table allows users to sort the address by the packet types and port.

Packet Types: Management Unicast means MAC address of the switch. It belongs to CPU port only. **Static Unicast** MAC address can be added and deleted. **Dynamic Unicast** MAC is MAC address learnt by the switch Fabric. **Static Multicast** can be added by CLI and can be deleted by Web and CLI. **Dynamic Multicast** will appear after you enabled IGMP and the switch learnt IGMP report.

Click on **Remove** to remove the static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.

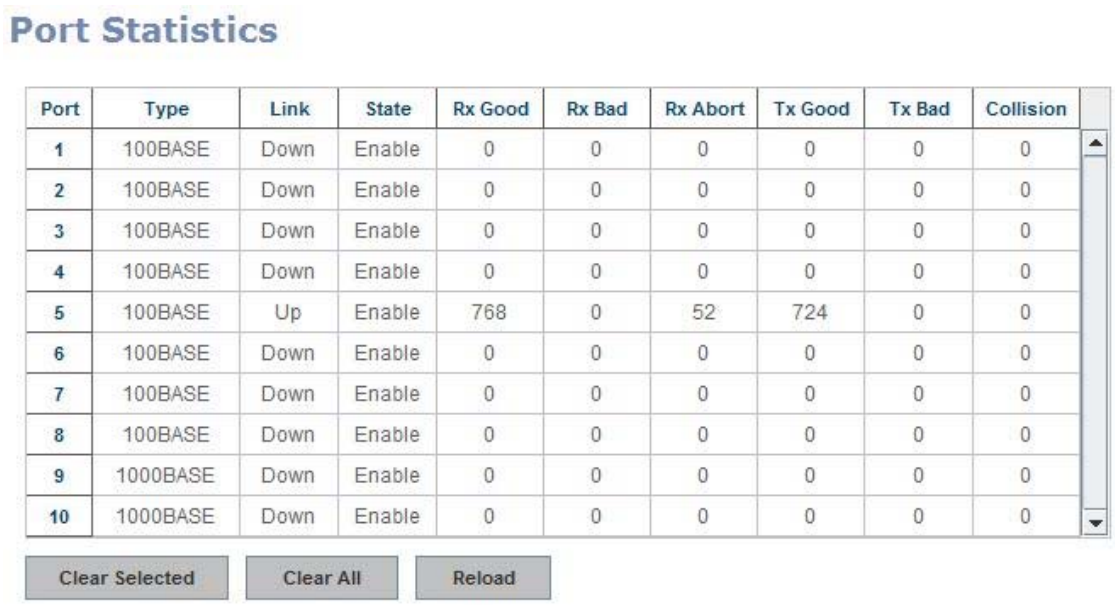


4.13.2 Port Statistics

In this page, you can view operation statistics for each port. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision. Rx means the received packet while Tx means the transmitted packets.

Note: If you see many Bad, Abort or Collision counts increased, that may mean your network cable is not connected well, the network performance of the port is poor…etc. Please check your network cable, Network Interface Card of the connected device, the network application, or reallocate the network traffic…etc.

Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.


Port Statistics
Port Type Link State Rx Good Rx Bad Rx Abort Tx Good Tx Bad Collision
1 100BASE Down Enable 0 0 0 0 0 0
2 100BASE Down Enable 0 0 0 0 0 0
3 100BASE Down Enable 0 0 0 0 0 0
4 100BASE Down Enable 0 0 0 0 0 0
5 100BASE Up Enable 768 0 52 724 0 0
6 100BASE Down Enable 0 0 0 0 0 0
7 100BASE Down Enable 0 0 0 0 0 0
8 100BASE Down Enable 0 0 0 0 0 0
9 1000BASE Down Enable 0 0 0 0 0 0
10 1000BASE Down Enable 0 0 0 0 0 0
Clear Selected
Clear All
Reload

4.13.3 Port Mirroring

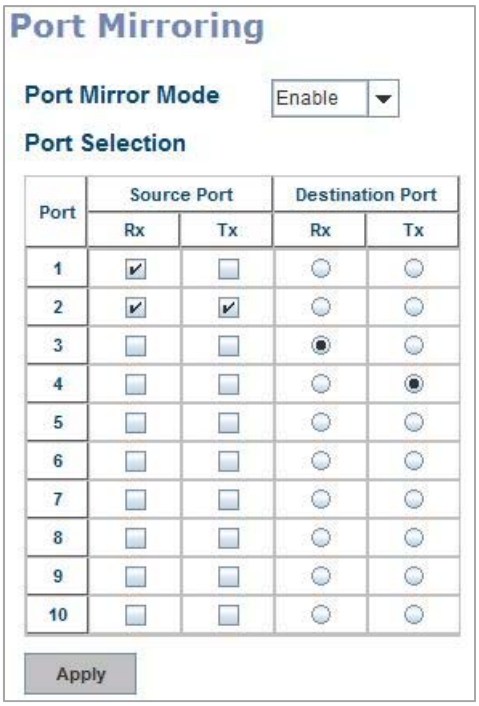
Port mirroring (also called port spanning) is a tool that allows you to mirror the traffic from one or more ports onto another port, without disrupting the flow of traffic on the original port. Any traffic that goes into or out of the Source Port(s) will be duplicated at the Destination Port. This traffic can then be analyzed at the Destination port using a monitoring device or application. A network administrator will typically utilize this tool for diagnostics, debugging, or fending off attacks.

Port Mirror Mode: Select Enable/Disable to enable/disable Port Mirror.

Source Port: This is also known as Monitor Port. These are the ports you want to monitor. The traffic of all source/monitor ports will be copied to destination/analysis ports. You can choose a single port, or any combination of ports, but you can only monitor them in Rx or TX only. Click on checkbox of the Port ID, RX, Tx or Both to select the source ports.

Destination Port: This is also known as Analysis Port. You can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port(s) being monitored. Only one RX/TX of the destination port can be selected. A network administrator would typically connect a LAN analyzer or Netxray device to this port.

Once you finish configuring the settings, click on **Apply** to apply the settings.



4.13.4 Event Log

In the 4.11.3, we have introduced System Log feature. When System Log Local mode is selected, PMI Switch will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data and time and content of the events.

Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.

4.13.5 Topology Discovery

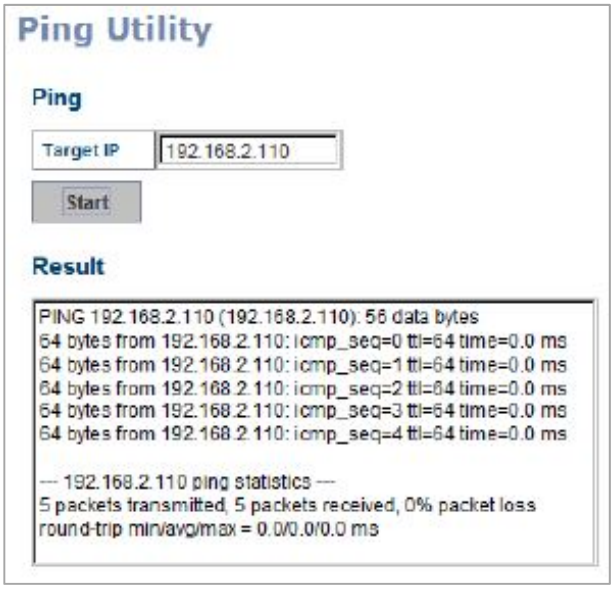
PMI Managed Switch support network topology discovery or LLDP (IEEE 802.1AB Link Layer Discovery Protocol) function that can help user to discovery multi-vendor's network devicec on same segment by NMS system which supports LLDP function; With LLDP function, NMS can easier maintain the topology map, display port ID, port description, system description, VLAN ID… Once the link failure, the topology change events can be updated to the NMS as well. The LLDP Port State can display the neighbor ID and IP leant from the connected devices.

The configuration and settings explain as following.

LLDP: Select Enable/Disable to enable/disable LLDP function.
LLDP Configuration: To configure the related timer of LLDP.
LLDP Timer: the interval time of each LLDP and counts in second; the valid number is from 5 to 254, default is 30 seconds.
LLDP Hold time: The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time. The default is 120 seconds.
Local port: the current port number that linked with neighbor network device.
Neighbor ID: the MAC address of neighbor device on the same network segment.
Neighbor IP: the IP address of neighbor device on the same network segment.
Neighbor VID: the VLAN ID of neightbor device on the same network segment.

4.13.6 Ping Utility

This page provides **Ping Utility** for users to ping remote device and check whether the device is alive or not. Type **Target IP** address of the target device and click on **Start** to start the ping. After few seconds, you can see the result in the **Result** field.


Ping Utility
Ping
Target IP
192.168.2.110
Start
Result
PING 192.168.2.110 (192.168.2.110): 56 data bytes
64 bytes from 192.168.2.110: icmp_seq=0 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=1 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=2 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=3 ttl=64 time=0.0 ms
64 bytes from 192.168.2.110: icmp_seq=4 ttl=64 time=0.0 ms
--- 192.168.2.110 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

4.13.7 CLI Commands of the Monitor and Diag

Command Lines of the Monitor and Diag configuration

Feature	Command Line
MAC Address Table	
Ageing Time	Switch(config)# mac-address-table aging-time 350 mac-address-table aging-time set ok! *Note: 350 is the new ageing timeout value.*
Add Static Unicast MAC address	Switch(config)# mac-address-table static 0012.7701.0101 vlan 1 interface fastethernet7 mac-address-table ucast static set ok!

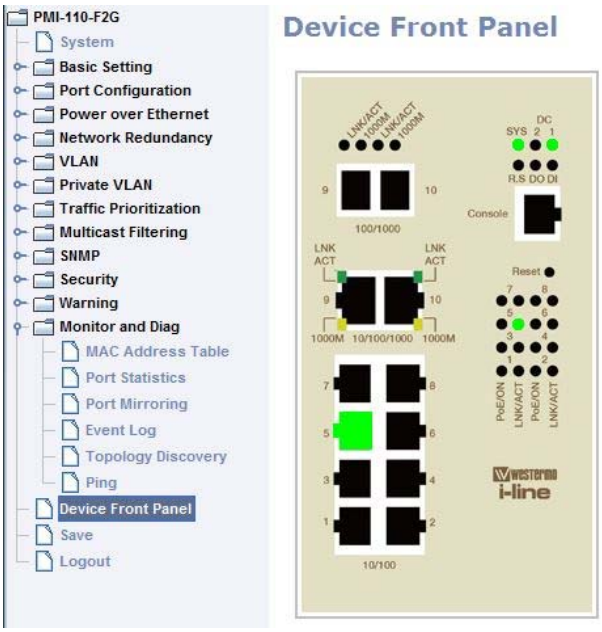
	Note: rule: mac-address-table static MAC_address VLAN VID interface interface_name
Add Multicast MAC address	Switch(config)# mac-address-table multicast 0100.5e01.0101 vlan 1 interface fa6-7 Adds an entry in the multicast table ok! ***Note: rule: mac-address-table multicast MAC_address VLAN VID interface_list interface_name/range***
Show MAC Address Table – All types	Switch# show mac-address-table ***** UNICAST MAC ADDRESS ***** Destination Address Address Type Vlan Destination Port ------------------- ---------- ------- ---------- 000f.b079.ca3b Dynamic 1 fa4 0012.7701.0386 Dynamic 1 fa7 0012.7710.0101 Static 1 fa7 0012.7710.0102 Static 1 fa7 0012.77ff.0100 Management 1 ***** MULTICAST MAC ADDRESS ***** Vlan Mac Address COS Status Ports ---- ---------- ---- ------- ---------- 1 0100.5e40.0800 0 fa6 1 0100.5e7f.fffa 0 fa4,fa6
Show MAC Address Table – Dynamic Learnt MAC addresses	Switch# show mac-address-table dynamic Destination Address Address Type Vlan Destination Port ------------------- ---------- ------- ---------- 000f.b079.ca3b Dynamic 1 fa4 0012.7701.0386 Dynamic 1 fa7
Show MAC Address Table – Multicast MAC addresses	Switch# show mac-address-table multicast Vlan Mac Address COS Status Ports ---- ---------- ---- ------- ---------- 1 0100.5e40.0800 0 fa6-7 1 0100.5e7f.fffa 0 fa4,fa6-7
Show MAC Address Table – Static MAC addresses	Switch# show mac-address-table static Destination Address Address Type Vlan Destination Port ------------------- ---------- ------- ---------- 0012.7710.0101 Static 1 fa7 0012.7710.0102 Static 1 fa7
Show Aging timeout time	Switch# show mac-address-table aging-time the mac-address-table aging-time is 300 sec.
Port Statistics	
Port Statistics	Switch# show rmon statistics fa4 (select interface) Interface fastethernet4 is enable connected, which has Inbound: Good Octets: 178792, Bad Octets: 0 Unicast: 598, Broadcast: 1764, Multicast: 160 Pause: 0, Undersize: 0, Fragments: 0 Oversize: 0, Jabbers: 0, Disacrds: 0 Filtered: 0, RxError: 0, FCSError: 0 Outbound: Good Octets: 330500 Unicast: 602, Broadcast: 1, Multicast: 2261 Pause: 0, Deferred: 0, Collisions: 0 SingleCollision: 0, MultipleCollision: 0 ExcessiveCollision: 0, LateCollision: 0 Filtered: 0, FCSError: 0

	Number of frames received and transmitted with a length of: 64: 2388, 65to127: 142, 128to255: 11 256to511: 64, 512to1023: 10, 1024toMaxSize: 42
Port Mirroring	
Enable Port Mirror	Switch(config)# mirror en Mirror set enable ok.
Disable Port Mirror	Switch(config)# mirror disable Mirror set disable ok.
Select Source Port	Switch(config)# mirror source fa1-2 both Received and transmitted traffic rx Received traffic tx Transmitted traffic Switch(config)# mirror source fa1-2 both Mirror source fa1-2 both set ok. ***Note: Select source port list and TX/RX/Both mode.***
Select Destination Port	Switch(config)# mirror destination fa6 both Mirror destination fa6 both set ok
Display	Switch# show mirror Mirror Status : Enabled Ingress Monitor Destination Port : fa6 Egress Monitor Destination Port : fa6 Ingress Source Ports :fa1,fa2, Egress Source Ports :fa1,fa2,
Event Log	
Display	Switch# show event-log <1>Jan 1 02:50:47 snmpd[101]: Event: Link 4 Down. <2>Jan 1 02:50:50 snmpd[101]: Event: Link 5 Up. <3>Jan 1 02:50:51 snmpd[101]: Event: Link 5 Down. <4>Jan 1 02:50:53 snmpd[101]: Event: Link 4 Up.
Ping	
Ping IP	Switch# ping 192.168.2.33 PING 192.168.2.33 (192.168.2.33): 56 data bytes 64 bytes from 192.168.2.33: icmp_seq=0 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=1 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=2 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=3 ttl=128 time=0.0 ms 64 bytes from 192.168.2.33: icmp_seq=4 ttl=128 time=0.0 ms --- 192.168.2.33 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

4.14 Device Front Panel

Device Front Panel commands allows you to see LED status of the switch. You can see LED and link status of the Power, DO, R.M. and Ports.

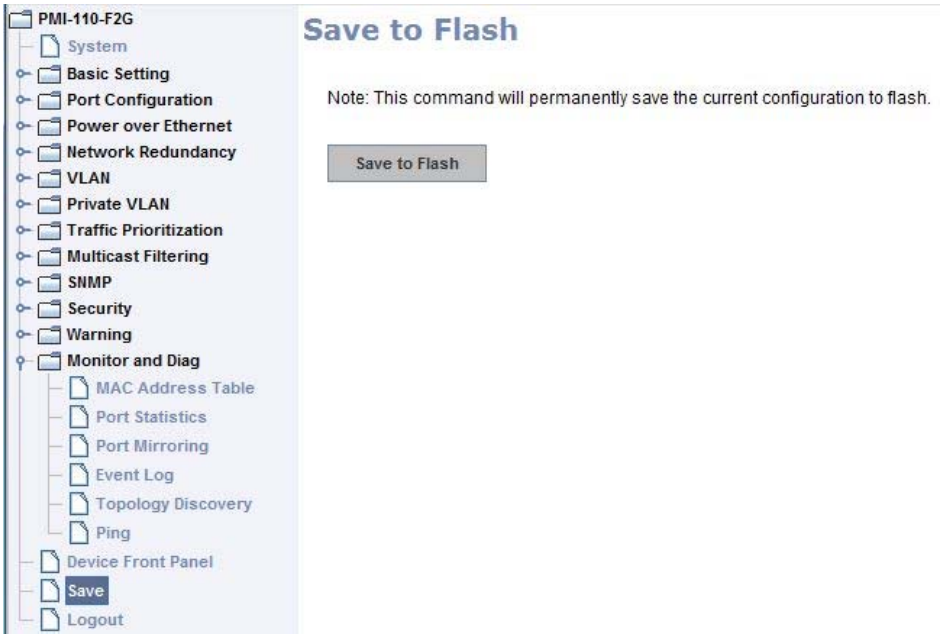
Feature	LED On	LED Blinking	LED off
Power	Power is on applying	Not avaliable	No power
Sys	System ready	System is on progress firmware upgrade or not ready	System not ready
R.S.	Green on: switch is working as ring master	Red blinking: Ring failed	Switch is working at slave mode.
Alarm	Green on: alarm relay active and contacts is short.	Not avaliable	Green off: relay output contact is open.
LNK/ACT	Port is linked	Port is on transmitting	Port is link down
1000M	The port is linked at 1000Mbps speed.	Not avaliable	Not avaliable
PoE	Green on: powering	On detecting	Power output over current or cable short



Note: No CLI command for this feature.

4.15 Save to Flash

Save Configuration allows you to save any configuration you just made to the Flash. Powering off the switch without clicking on **Save Configuration** will cause loss of new settings. After selecting **Save Configuration**, click on **Save to Flash** to save your new configuration.



Command Lines:

Feature	Command Line
Save	SWITCH# write Building Configuration… [OK] Switch# copy running-config startup-config Building Configuration... [OK]

4.16 Logout

The switch provides 2 logout methods. The web connection will be logged out if you don't input any command after 30 seconds. The Logout command allows you to manually logout the web connection. Click on **Yes** to logout, **No** to go back the configuration page. (refer to following diagram)

Command Lines:

Feature	Command Line
Logout	SWITCH> exit SWITCH# exit

5 Appendix

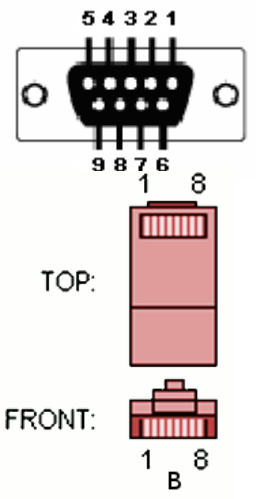
5.1 Pin assignment of RS-232 serial console cable

The RS-232 console cabl include in the unitbox, and the connectors are RJ-45 and DB-9 female.

The following diagram showns the pins assignment of RJ-5 and DB-9 female connectors.

RJ-45 Pin	DB-9 Pin	Description
1	8	N/A
2	9	N/A
3	**2**	**TxD**
4	1	N/A
5	**5**	**GND**
6	**3**	**RxD**
7	4	N/A
8	7	N/A

DB-9 Female Connector



5.2 Westermo Private MIB

Westermo provides many standard MIBs for users to configure or monitor the switch's configuration by SNMP. But, since some commands can't be found in standard MIB, Westermo provides Private MIB to meet up the need. Compile the private MIB file by your SNMP tool. You can then use it. Private MIB can be found in product CD or downloaded from Westermo Web site.

Private MIB tree is the same as the web tree. This is easier to understand and use. If you are not familiar with standard MIB, you can directly use private MIB to manage /monitor the switch, no need to learn or find where the OIDs of the commands are.

5.3 Revision History

Edition	Date	Modifications
V0.1	2014/03/28	The first draft release

Westermo • SE-640 40 Stora Sundby, Sweden
Tel +46 16 42 80 00 Fax +46 16 42 80 01
E-mail: info@westermo.com
www.westermo.com

Sales Units

Westermo Data Communications

China
sales.cn@westermo.com
www.cn.westermo.com

France
infos@westermo.fr
www.westermo.fr

Germany
info@westermo.de
www.westermo.de

North America
info@westermo.com
www.westermo.com

Singapore
sales@westermo.com.sg
www.westermo.com

Sweden
info.sverige@westermo.se
www.westermo.se

United Kingdom
sales@westermo.co.uk
www.westermo.co.uk

Other Offices

For complete contact information, please visit our website at www.westermo.com/contact or scan the QR code with your mobile phone.